# Blockchain en smart contracts

Goossens, Jurgen; Verslype, Kristof; Tjong Tjin Tai, Eric

*Publication date:*
2020

*Document Version*
Peer reviewed version

**Blockchain en smart contracts**

# Blockchain en smart contracts

Herijking van de rol van de vertrouwde tussenpersoon in de algoritmische samenleving

Jurgen Goossens
Kristof Verslype
Eric Tjong Tjin Tai

Meer informatie over deze en andere uitgaven kunt u verkrijgen bij:

Sdu Klantenservice
tel.: 070 – 378 98 80
e-mail: info@sdu.nl
web: www.sdu.nl/service

Vormgeving omslag: Villa Y, Henxel
Zetwerk: Imago Mediabuilders, Amersfoort

ISBN: 978 9012 40585 0
NUR: 826

# Inhoudsopgave

# 1. Inleiding

*'Blockchain is a foundational technology: It has the potential to create new foundations for our economic and social systems. But while the impact will be enormous, it will take decades for blockchain to seep into our economic and social infrastructure.'*[1]

Marco Iansiti en Karim Lakhani, *Harvard Business Review* (2017)

## 1.1. Probleemstelling

Een samenleving zonder internet is tegenwoordig ondenkbaar. Toen het protocol waarop internet gebouwd is (TCP/IP) midden de jaren 1970 ontwikkeld werd, kon niemand de impact door het ontwikkelen van allerhande internetapplicaties voorspellen. Denk bijvoorbeeld aan eBay, Facebook, Google Search, YouTube, Netflix, Skype en internetbankieren. Er zijn daarnaast ook talloze bedrijfsprocessen waar de burger niet rechtstreeks mee in contact komt. Al deze applicaties zijn in essentie gebaseerd op één simpel principe, namelijk snel en goedkoop *informatie* uitwisselen.
Blockchain, dat voor het eerst in Bitcoin toegepast werd, belooft hetzelfde, maar deze keer vooral voor het uitwisselen van *waarde*. Zoals e-mail als de applicatie wordt beschouwd die internet deed *boomen*, kan in zekere zin voor blockchain hetzelfde worden verteld over Bitcoin. Op zijn minst is Bitcoin verantwoordelijk voor de blockchainhype, waardoor iedereen nu in elk geval al eens van blockchain gehoord heeft. Wat internet nu betekent voor de uitwisseling van gegevens, zou blockchain kunnen betekenen voor het uitwisselen van waarde. Blockchain maakt het immers mogelijk om snel, goedkoop, geautomatiseerd en zonder tussenpartij waarde uit te wisselen.
In de *Harvard Business Review* verscheen in 2017 een artikel waarin de auteurs stellen dat blockchain een *grondleggende* technologie is, net zoals internet of elektriciteit[2]. Dit betekent dat blockchain een ingrijpende impact kan hebben in niet één, maar in verscheidene domeinen van de samenleving. Blockchain wordt dan ook het potentieel toegeschreven om nieuwe fundamenten voor het economisch en sociaal systeem te leggen. Hoewel een enorm potentieel aan de technologie toegeschreven wordt, zal het nog een hele tijd duren vooraleer blockchain fundamenteel op onze economische en

1 M. Iansiti & R. Lakhani, 'The Truth About Blockchain', *Harvard Business Review*, januari-februari 2017, https://hbr.org/2017/01/the-truth-about-blockchain.
2 *Ibid.*

maatschappelijke structuren zal inwerken, net zoals elektriciteit en het internetprotocol TCP/IP.

Internet heeft ondertussen ook al geleid tot een grote impact op onze wetgeving. Denk aan de Algemene Verordening Gegevensbescherming of de regels rond elektronische handel en financiële dienstverlening. Indien blockchain haar beloftes waarmaakt, zal ook deze nieuwe technologie na verloop van tijd nieuwe regelgeving kunnen noodzaken. Op zijn minst zal op korte termijn waar mogelijk een teleologische, pragmatische interpretatie van bestaande wettelijke regels moeten worden gehanteerd. Zo kan het doel van bestaande regelgeving worden gewaarborgd, ook wanneer gebruik zou worden gemaakt van blockchain, bijvoorbeeld bij transacties of overheidsbesluiten.

Voor juristen is de technologie ook van belang, aangezien het mogelijk hun dagelijkse beroepspraktijk grondig zou kunnen veranderen. Volgens sommige geluiden zouden bijvoorbeeld notarissen, overheidsorganen en banken zelfs overbodig kunnen worden. Hoewel dergelijke stellingen natuurlijk bijzonder ongenuanceerd en onrealistisch zijn, wordt wel verwacht dat de impact van deze technologie ingrijpend zal zijn. Dit boek biedt een juridisch, technisch én maatschappelijk overzicht van deze nieuwe technologie. Door de intensieve, interdisciplinaire samenwerking tussen een publiekrechtelijke jurist (Jurgen Goossens), een computerwetenschapper/cryptograaf (Kristof Verslype), en een privaatrechtelijke jurist/ingenieur informatica (Eric Tjong Tjin Tai) geeft het boek een unieke analyse van de uitdagingen, mogelijkheden en beperkingen van blockchain en smart contracts. Het boek geeft u gedegen inzicht en bereidt u voor op de toekomstmogelijkheden van blockchain en smart contracts. Het boek is een actualisatie van het boek van J. Goossens en K. Verslype, *Blockchain en smart contracts. Het einde van de vertrouwde tussenpersoon?*, Brussel: Larcier, 2018. De tekst werd grondig inhoudelijk aangepast voor de Nederlandse markt en werd geüpdatet naar aanleiding van de nieuwste ontwikkelingen en inzichten. Daarnaast werd een derde coauteur, T.F.E. Tjong Tjin Tai, betrokken en bevat het boek nu een volledig nieuw hoofdstuk over blockchain en vastgoed.

Na deze inleiding volgen nog zeven andere hoofdstukken. Hoofdstuk 2 gaat over smart contracts, waarmee het blockchainnetwerk regels collectief kan afdwingen. Hoofdstuk 3 gaat in op bitcoins en andere virtuele munten, terwijl hoofdstuk 4 de mogelijke toepassing van blockchain in de vastgoedpraktijk analyseert. Hoofdstuk 5 behandelt beknopt allerlei andere blockchaintoepassingen. Hoofdstuk 6 gaat in op de toepasselijke privacywetgeving, waarna hoofdstuk 7 dieper ingaat op het concept van gedistribueerd vertrouwen. Hoofdstuk 8, ten slotte, beoogt uit de opkomst en de ontwikkeling van internet enkele lessen te trekken voor de toekomst van blockchain.

We stellen eerst de auteurs nog even voor en beschrijven daarbij kort hun expertise met betrekking tot blockchain en smart contracts.

Jurgen Goossens is universitair hoofddocent staats- en bestuursrecht aan Tilburg University. Hij is projectleider van het NWO-MVI gefinancierd onderzoek (2020-2024) over blockchaintoepassingen van de overheid: 'Blockchain in de netwerksamenleving. Op zoek naar transparantie, vertrouwen en legitimiteit', waarbinnen dit boek mede is tot stand gekomen. Zijn onderzoeksexpertise heeft betrekking op de verhouding bur-

ger-overheid. Hij richt zich op 1° de complexiteit en hyperconnectiviteit die ontstaan door het gebruik van algoritmen, zoals smart contracts, en gedistribueerde technologieën, zoals blockchain, 2° effectieve rechtsbescherming van de burger tegen de overheid en 3° burgerparticipatie.
Kristof Verslype is doctor in de ingenieurswetenschappen (KU Leuven). Hij onderzocht hoe privacy verbeterd kan worden met behulp van cryptografie. Hij werkt dagelijks met cryptografie en blockchaintechnologie als onderzoeker en adviseur bij Smals, een ICT-dienstverlener voor overheidsinstellingen. Hij heeft daarbij vanuit zijn academische achtergrond een sterke focus op privacy en veiligheid.
Eric Tjong Tjin Tai is hoogleraar privaatrecht aan Tilburg University. Hij is tevens ingenieur Informatica (TU Delft). De afgelopen jaren heeft hij herhaaldelijk geschreven over juridische aspecten van blockchain en smart contracts, onder meer in het KNB Preadvies 2018 en als medeonderzoeker voor het WODC rapport Blockchain en het recht (2019).
In tegenstelling tot verschillende andere bijdragen over dit thema, focussen wij weinig tot niet op wat de technologie belooft. We beschouwen onszelf niet als visionairs en voelen allerminst de behoefte om in geuren en kleuren te beschrijven hoe fantastisch de toekomst met blockchain eruit zou kunnen zien. Visionairs zitten er geregeld immers al eens stevig naast. Wij vertrekken vanuit de concrete, bestaande praktijkervaringen van vandaag en zullen daarbij een realistische, eerder dan futuristische benadering hanteren. Desondanks willen we toch eerst hierna duiden waarom er zo een hype is ontstaan rond blockchain.

## 1.2. Impact van blockchain

De in 2009 gelanceerde Bitcoin is de eerste en meest populaire toepassing die onderliggend de blockchaintechnologie gebruikt. Bitcoin laat toe om digitaal waarde, zogenaamde *virtuele munten* of *cryptomunten*, te creëren en te verhandelen zonder een intermediaire tussenpersoon, zoals een bank. Bitcoin werd in 2008[3] beschreven door iemand of een groep van mensen, die we enkel kennen onder het pseudoniem Satoshi Nakamoto, wat natuurlijk bijdraagt aan het mythische imago van Bitcoin.
Al vrij snel werd duidelijk dat de technologie gebruikt kan worden om ook in heel wat andere toepassingen en domeinen de afhankelijkheid van het optreden van intermediaire partijen omwille van de noodzaak aan vertrouwen te reduceren en zelfs volledig weg te nemen. Blockchain wordt dan ook gezien als een technologie voor *disintermediatie*. Allerlei handelingen die vandaag de dag een tussenpartij vereisen, zouden dankzij blockchain ook zonder deze tussenpartij mogelijk worden. Blockchain, of de ruimere term *Distributed Ledger Technology* (DLT) (gedistribueerd grootboek technologie), beoogt dus de tussenkomst van *Trusted Third Parties* (TTP) (vertrouwde tussenpersonen) overbodig te maken.

3 N. Satoshi, *Bitcoin: A peer-to-peer electronic cash system*, 2008, https://bitcoin.org/bitcoin.pdf.

De volgende voorbeelden verduidelijken hoe hypothetisch een 'ultieme' blockchain-toekomst eruit zou kunnen zien. Het is, samengevat, een toekomst zonder intermediaire partijen of – in onze realistische visie – een toekomst waarin de rol van bijvoorbeeld notarissen, commerciële internetplatformen, beheerders, banken of overheden wordt herijkt.

### 1.2.1. *Notarissen en het Kadaster*

De notaris en het Kadaster moeten eraan geloven volgens de *blockchainbelievers*. Burgers zullen zonder rol voor de notaris en het Kadaster zelf aktes kunnen registreren in de blockchain. Op het moment dat deze registratie plaatsvindt, zijn de levering en de registratiedatum onwijzigbaar en hebben we garanties over de identiteit van de ondertekenaars. Aktes zoals verkoopovereenkomsten, huwelijkscontracten, testamenten en oprichtingsakten kunnen zo rechtstreeks geregistreerd worden zonder tussenkomst van een derde partij en dus zonder aanzienlijke notariskosten. Het transfereren van vastgoed zal rechtstreeks tussen koper en verkoper kunnen gebeuren. De blockchain-gebaseerde smart contracttechnologie kan het voldoen aan bepaalde regels en voorwaarden afdwingen. In de ideale wereld van de *blockchainbelievers* wordt het juridische bewijs van de overdracht van een goed dus niet langer verbonden aan de tussenkomst van een notaris en de registratie door het Kadaster, maar aan de loutere opname in de blockchain. Het Kadaster moet nu de registratie van stukken weigeren die niet voldoen aan de wettelijke eisen (art. 3:19 en 3:20 BW), waardoor de inhoudelijke kwaliteit van het register wordt gewaarborgd. Deze functie zou volgens *blockchainbelievers* kunnen worden overgenomen door blokchain en smart contracts.
Blockchain zou bovendien het administratieve deel van het werk van een notaris efficiënter kunnen laten verlopen, waardoor er meer tijd vrij zal komen voor de intellectueel uitdagendere taak van advisering. Voor het zover is, moeten wettelijk gezien natuurlijk partijen eerst zelf aktes kunnen opstellen en deze in het register kunnen laten inschrijven. De Nederlandse wetgever heeft er immers voor geopteerd om de levering van onroerend goed alleen te laten plaatsvinden met een notariële akte (art. 3:89 BW), en dus een akte die door een notaris is opgesteld.[4] Daarnaast is de notaris ook verplicht om te zorgen voor allerlei andere dingen.[5] Hij moet bijvoorbeeld controleren op de identiteit en wilsbekwaamheid van partijen, nagaan of partijen echt begrijpen wat er gaat gebeuren en controles uitvoeren op verdachte transacties zoals witwassen. Verder gaat hij na of het onroerend goed daadwerkelijk geleverd kan worden, namelijk of er geen beslag op rust en of er niet nog hypotheekrechten of andere beperkingen op rusten. Tot slot heeft de notaris vaak een rol in de afwikkeling van betalingsverkeer rond

4 Zie hierover T.F.E. Tjong Tjin Tai, 'De blockchain als alternatief voor de notariële praktijk', in: F.W.J.M. Schols & B.C.M. Waaijer (red.), *Financiële zorgplicht van de notaris*, preadviezen KNB 2018, Den Haag: Sdu 2018, p. 99-135.

5 *Ibid.*; J.C.H. Melis & B.C.M. Waaijer, *De Notariswet*, 9e dr., Deventer: Wolters Kluwer 2019; H.W. Heyman, S.E. Bartels & V. Tweehuysen, *Vastgoedtransacties. Overdracht*, Den Haag: Boom juridisch 2019.

de transactie.[6] In hoofdstuk 4, Blockchain en vastgoed gaan we veel dieper op in op de mogelijke functies die blockchain zou kunnen vervullen bij de overdracht van onroerende goederen.

### 1.2.2. *Commerciële platformen*

Volgens *blockchainbelievers* zouden allerlei andere centrale entiteiten, zoals gecentraliseerde, commerciële internetplatformen overbodig worden. Denk daarbij onder andere aan sociale netwerken zoals Facebook, Instagram, Twitter, LinkedIn en Snapchat; diensten voor opslag, delen en synchronisatie van bestanden zoals Google Drive en Dropbox; verhuur-, verkoop-, en veilingplatformen zoals Airbnb, booking.com, huizenzoeker.nl, Amazon en eBay; en talloze andere platformen zoals datingsites, Kickstarter (crowdfunding), Uber en Deliveroo.

### 1.2.3. *Beheerders*

In dezelfde logica zouden op weg naar de blockchainwereld ook alle centrale beheerders eraan geloven. Denk daarbij onder meer aan beheerders van domeinnamen en auteursrechten.
Domeinnamen zoals sdu.nl worden nog steeds beheerd door een hiërarchische top-downstructuur met helemaal bovenaan het in de Verenigde Staten gebaseerde *ICANN*. Deze organisatie heeft bijvoorbeeld SIDN (Stichting Internet Domeinregistratie Nederland) het recht gegeven alle domeinnamen die eindigen op .nl te beheren. In de blockchaintoekomst zouden deze partijen niet langer nodig zijn.
Het transfereren van auteursrechten, het innen van royalty's en het uitkeren ervan aan de artiesten zou mogelijk worden zonder centrale instantie zoals Buma/Stemra[7].

### 1.2.4. *Banken*

Het verrichten van financiële transacties en dus de overdracht van waarde over het internet wordt mogelijk zonder bank en zonder enige vorm van overheidstoezicht of -controle. Betalingen, vooral internationaal, zouden daardoor een stuk goedkoper worden. Ook andere taken die vandaag de dag een bank vereisen, zoals het deponeren en het vrijgeven van de huurwaarborg, zouden voortaan kunnen plaatsvinden zonder bank. Volgens sommigen worden zelfs centrale banken overbodig[8].

---

6 F.W.J.M. Schols & B.C.M. Waaijer (red.), *Financiële zorgplicht van de notaris*, preadviezen KNB 2018, Den Haag: Sdu 2018.

7 Zie uitgebreid G. Gürkaynak, I. Yilmaz, B. Yesilaltay & B. Bengi, 'Intellectual property law and practice in the blockchain realm', *Computer Law & Security Review* 2018, nr. 34, p. 847-862.

8 J.E. McWhinney, 'Can Bitcoin Kill Central Banks?', 30 september 2018, www.investopedia.com/articles/investing/050715/can-bitcoin-kill-central-banks.asp.

### 1.2.5. *Overheden*

Een aantal van de kerntaken van de overheid zijn het innen en het besteden van belastingen, het afdwingbaar maken van verbintenissen, namelijk via gerechtelijke afdwinging van de uitvoering daarvan, het beschermen van private eigendom en het organiseren van verkiezingen. Blockchainadepten propageren dat de overheid voor elk van deze aspecten overbodig wordt in de toekomst.
Het innen van belastingen en het besteden ervan, bijvoorbeeld in het kader van de sociale zekerheid, gebeurt in een blockchainwereld aan de hand van vooraf bepaalde regels, waarbij het blockchainnetwerk collectief garandeert dat deze regels gerespecteerd worden. Dit gebeurt bovendien transparant, zodat de burger kan verifiëren wat er met zijn of haar betaalde belastingen gebeurt.
Sommige overeenkomsten kunnen automatisch worden uitgevoerd waarbij een blockchainnetwerk de correcte uitvoering afdwingt. Betwisting van de uitvoering van juridische overeenkomsten wordt in beginsel onmogelijk, waardoor een rechter niet langer nodig zou zijn. Denk hierbij bijvoorbeeld aan een verzekeringscontract dat vliegtuigpassagiers automatisch een vergoeding betaalt indien er een bepaalde vluchtvertraging is. De rol van de staat die nodig is om overeenkomsten tussen contracterende partijen af te dwingen bij niet-uitvoering en geschillen hieromtrent te beslechten, verdwijnt dus. In de praktijk zal het natuurlijk niet in alle gevallen zo simpel zijn en zal bijvoorbeeld het recht op een eerlijk proces en een daadwerkelijk rechtsmiddel gewaarborgd moeten zijn in het licht van de artikelen 6 en 13 van het Europees Verdrag voor de Rechten van de Mens (hierna EVRM).
In een goed functionerende democratische rechtsstaat organiseert de overheid op geregelde tijdstippen verkiezingen. In een wereld waarbij we stemmen via blockchain, zou de kans op fraude in het stemlokaal nihil worden. Geen enkele partij zal de verkiezingsresultaten nog kunnen vervalsen. Er zullen dus niet langer getuigen, internationale waarnemers of hertellingen nodig zijn. Het organiseren van digitale verkiezingen is sowieso echter al controversieel, *a fortiori* wanneer daarbij gebruik zou worden gemaakt van een technologie die op gespannen voet staat met de privacywetgeving (*infra* hoofdstuk 6, Privacywetgeving)[9].
In de Nederlandse gemeente Groningen heeft men al geëxperimenteerd met blockchain bij het tellen van de stemmen over het referendum met betrekking tot de Wet op de inlichtingen- en veiligheidsdiensten[10]. In de Zwitserse stad Zug heeft men eveneens de kiezers laten stemmen via blockchain en de daar ingevoerde digitale identiteit[11]. Deze stad ligt in de zogenaamde 'Cryptovalley'. Door de ingevoerde regulering en ondersteuning vanuit de overheid zijn talrijke blockchainorganisaties zoals Ethereum en

9 C. Lagarde, 'Addressing the Dark Side of the Crypto World', *IMF Blog*, 13 maart 2018, https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world.
10 Zie 'Proef stemmen tellen met blockchain afgerond', 22 maart 2018, www.berenschot.nl/actueel/2018/maart/stemmen-met-blockchain en https://stemmen-telt.nl/groningen/#pilot.
11 Zie 'Switzerland's first municipal blockchain vote hailed a success', 2 juli 2018, www.swissinfo.ch/eng/business/crypto-valley-_-switzerland-s-first-municipal-blockchain-vote-hailed-a-success/44230928.

Cardano hier ontstaan. Onderzoek met betrekking tot het gebruik van blockchain bij de Nederlandse verkiezingen leidt tot de conclusie dat het stemgeheim bij verkiezingen zoals voorzien door artikel 53, lid 2 van de Grondwet op dit moment nog niet voldoende gewaarborgd kan worden, aangezien bij blockchain in beginsel elke transactie gevolgd kan worden[12]. Hoepman concludeert om verschillende redenen dat de toepassing van blockchaintechnologie in het verkiezingsproces niet wenselijk is.

### 1.2.6. *De rol van trusted third parties*

Waarom zouden we ons in een blockchainavontuur storten en bovenstaande tussenpartijen overbodig maken? De kritiek op deze *trusted third parties* is tweeledig: hoge kosten en een suboptimaal niveau van vertrouwen. Veel van deze tussenpartijen wordt verweten te duur te zijn. Dit zou het gevolg zijn van inefficiëntie of (quasi-)monopolieposities, waardoor ze in staat zijn disproportioneel hoge vergoedingen in rekening te brengen. Blockchaintechnologie zou deze kosten, ook wel frictie genoemd, sterk verminderen.
Of we het nu willen of niet, we moeten die partijen ten volle kunnen vertrouwen en dat is niet steeds het geval. We moeten de bank vertrouwen veilig met ons geld om te gaan, wat ondanks de depositogarantie niet evident bleek ten tijde van de bankencrisis. We moeten Facebook vertrouwen dat de gegevens die ze over ons hebben, niet misbruikt worden, zoals in het geval van Cambridge Analytica. De leden van Ashley Madison, een datingsite voor buitenechtelijke relaties, vertrouwden er ten onrechte tot de zomer van 2015 op dat hun gegevens niet op straat zouden belanden.

### 1.2.7. *The sky is the limit?*

Blockchain doet echter meer dan het overbodig maken van tussenpersonen. De technologie kan bijvoorbeeld de transparantie van allerlei praktische of industriële processen verbeteren, bijvoorbeeld de herkomst van voedsel en het afgelegde traject ervan (*infra* 5.4. Casus herkomst en toeleveringsketen). Hetzelfde is mogelijk voor onder meer wagens, diamanten, containers en afvalverwerking. Fraude wordt zo een stuk moeilijker. Transparantie is ook van bijzonder belang onder meer bij openbare aanbestedingen, het toekennen van subsidies of het overzicht van de al dan niet betaalde mandaten van een politicus. Om de transparantie in dergelijke processen te garanderen, is dankzij blockchain geen centrale partij nodig die alles bijhoudt en de correctheid garandeert.
Verder wordt blockchaintechnologie vooral ook gehanteerd als onderliggende technologie om smart contracts mogelijk te maken. Smart contracts (*infra* hoofdstuk 2, Smart contracts) zijn een set van toepassingsspecifieke regels, uitgedrukt in computercode,

12 J.-H. Hoepman, *Het gebruik van blockchain technologie in het verkiezingsproces*, Radboud Universiteit, PI.lab, 12 april 2018, https://www.rijksoverheid.nl/documenten/rapporten/2018/04/12/het-gebruik-van-blockchaintechnologie-in-het-verkiezingsproces.

die door het blockchainnetwerk collectief en correct uitgevoerd worden, waarbij het smart contract waarde kan ontvangen, blokkeren en transfereren. Dit laat toe om gedistribueerd, dus zonder centrale partij, afspraken tussen partijen af te dwingen. Een smart contract dwingt dus de toepassing af van de algoritmische regel '*if this, than that*'. Indien aan bepaalde voorwaarden wordt voldaan, vindt een bepaalde handeling of transactie plaats. Niemand kan eenzijdig impact hebben op de correcte uitvoering van de regel.

Dit laat conceptueel zelfs het ontstaan toe van bedrijven zonder fysiek adres, werkelijke managers of werknemers, waarbij de bedrijven autonoom beslissingen nemen. Alle logica van het bedrijf wordt collectief en transparant door het blockchainnetwerk uitgevoerd. In een eenvoudig voorbeeld zouden aandeelhouders kunnen stemmen in welke projecten geïnvesteerd wordt, wat vervolgens automatisch uitgevoerd wordt.

Een centraal idee in blockchain is dat iemand niet enkel zelf de eigenaar is van zijn activa, maar er zelf ook de volledige, autonome controle over heeft en op elk moment kan beslissen bezittingen ogenblikkelijk te transfereren.

Identiteits- en persoonsgegevens zijn voor burgers van bijzonder belang. Dankzij blockchain zou de burger, als eigenaar van deze gegevens (*self-sovereign identity*), zelf kunnen bepalen wie deze mag zien of gebruiken. Wie mag er zien dat ik meerderjarig ben? Welke arts krijgt toegang tot mijn medische gegevens, die in vele landen nu verspreid liggen in verschillende ziekenhuizen en bij verschillende dokters? Wie krijgt welke van mijn diploma's en onderwijscertificaten te zien? De burger heeft te allen tijde een volledig overzicht hiervan en kan desgewenst toegangsrechten wijzigen.

### 1.2.8. *Realistische benadering*

Bovenstaande – onvolledige – lijst is op zich al indrukwekkend en geeft een beeld van de enorme impact die de technologie zou kunnen hebben. Het schetst een mogelijke 'ultieme' blockchainwereld. Het achterliggende idee is dat door het elimineren van tussenpersonen allerlei processen sneller en goedkoper kunnen, wat uiteindelijk moet resulteren in een samenleving met minder frictie en dus een vlotter draaiende economie.

Er wordt enorm veel van blockchain verwacht, maar tegelijkertijd is het een technologie die vaak niet goed begrepen wordt. Dit kan paradoxaal klinken, maar het is juist doordat blockchain niet goed begrepen wordt dat de verwachtingen zo hoog liggen. Omwille van een gebrek aan voldoende kennis ziet men de tekortkomingen en de uitdagingen minder. *Believers* verkondigen weleens dat alle problemen binnen afzienbare tijd zullen worden opgelost, maar dit technologie-optimisme, dat we trouwens ook bijvoorbeeld bij Artificiële Intelligentie zien, gaat voorbij aan de realistische mogelijkheid van fundamentele beperkingen die niet gemakkelijk zijn weg te werken.

Een van de uitdagingen is het tegengaan van silovorming. Hiermee wordt bedoeld dat gegevens verspreid en onnodig gedupliceerd worden over verschillende, van elkaar geïsoleerde locaties of van elkaar geïsoleerde blockchains. Hoe behoudt de burger of de onderneming nog het overzicht? Het is ons niet helemaal duidelijk hoe blockchainnet-

werken op een generieke manier met elkaar kunnen communiceren zonder opnieuw intermediaire partijen te introduceren. Voor alle toepassingen een en dezelfde blockchain gebruiken, lijkt ons weinig realistisch.

Blockchain is een specifiek technologisch concept dat een idee populariseerde dat voorheen enkel onder cryptografen leefde, namelijk dat – vanuit een technologisch perspectief – alles wat mogelijk is met een centrale partij, ook zonder die centrale partij gedaan kan worden. Het onderscheid tussen het technologisch concept en dit idee wordt evenwel niet steeds voldoende gemaakt. Mede hierdoor gaapt er vandaag de dag een kloof tussen enerzijds de verwachtingen en anderzijds wat technologisch mogelijk is.

Misschien is blockchain slechts een tussenstadium in de richting van meer decentralisatie en (hyper)connectiviteit en zal de technologie die we uiteindelijk daarvoor zullen gebruiken, nog amper lijken op blockchain. Er zijn nu al technologieën die weliswaar bepaalde ideeën uit blockchain behouden, maar op zich geen blockchaintechnologie zijn. Voorbeelden zijn IOTA[13] en CORDA[14].

Blockchain populariseerde een idee dat een maatschappelijke impact en een ideologische dimensie heeft. Dankzij deze technologie is nu inderdaad meer aandacht voor de vraag of een intermediaire of centrale partij echt nog wel nodig is. Dat kan gaan van banken, multinationals, auteursrechtenverenigingen en notarissen tot overheden. In sommige gevallen kan vervolgens tot de conclusie worden gekomen dat ook zonder blockchain afhankelijkheidsrelaties gereduceerd kunnen worden. Misschien zou hier wel de grootste verdienste van de technologie kunnen liggen. Niet in de technologie zelf, maar in het idee dat het met zich meedraagt dat uiteindelijk misschien maar zelden effectief in de praktijk met blockchaintechnologie gerealiseerd zal worden.

Dat iets technologisch mogelijk is, impliceert trouwens nog niet dat het ook steeds maatschappelijk wenselijk is. In de loop van dit boek zullen we zien dat aan de huidige generatie blockchaintechnologieën, zoals Bitcoin en Ethereum, technische en juridische problemen verbonden zijn, die bij een onverstandig gebruik risico's met zich meebrengen. De risico's zullen mettertijd *by design* beter opgevangen moeten worden.

Ook ethisch zijn er belangrijke aandachtspunten, bijvoorbeeld groepen met een laag niveau van digitale geletterdheid en andere kwetsbare groepen. Organisatorisch en maatschappelijk zijn er ook uitdagingen. Indien alle bovenstaande voorbeelden zich effectief binnen een paar jaar realiseren, zouden de participanten in het netwerk in beginsel toezien op de correcte uitvoering van regels. Iemand moet natuurlijk deze regels vastleggen en, indien nodig, aanpassen. Bovendien zullen allerlei instanties informatie aan de blockchain moeten aanleveren. Ook deze instanties moeten vertrouwd worden en een vorm van toezicht lijkt dus wenselijk. Zelfs in de volmaakte blockchainwereld blijft er dus een overheid als leverancier van gegevens, regulator en toezichthouder. Enkel de rol van die vertrouwde tussenpersoon zal dus moeten worden herijkt in een wereld van hyperconnectiviteit gebaseerd op DLT en gebruik van algoritmen

13 www.iota.org/.
14 www.r3.com/.

zoals in dit geval smart contracts. De stelling dat door blockchain overheden en andere vertrouwde tussenpersonen volledig zullen verdwijnen, is dus erg ongenuanceerd. Het is trouwens de hedendaagse vertaling van een stelling die al enkele decennia de ronde doet, namelijk dat verschillende diensten vervangen zullen worden door computers. In een steeds complexer wordende samenleving waarin de overheid steeds meer regelt in elk domein van ons leven (evolutie van de nachtwakersstaat naar de socialeverzorgingsstaat), die heeft geleid tot opkomst van de zogenaamde *administrative state*[15] met verreikende bevoegdheden voor het bestuur, krijgt de overheid een steeds uitgebreider en complexer takenpakket. Mede dankzij technologie, waaronder blockchain en smart contracts, kan dit takenpakket beheersbaar worden gehouden. Blockchain zal de overheid echter nooit ontslaan van haar internationale, grondwettelijke en andere wettelijke verplichtingen. Op de overheid rusten immers naast negatieve ook positieve verplichtingen.

### 1.2.9. *Verwachtingen*

De verwachtingen lagen tijdens het hoogtepunt van de hype enorm hoog, zoals onder meer blijkt uit de exploderende beurswaarderingen van bedrijven die de term *blockchain* in hun naam opnemen. Toen Kodak bijvoorbeeld begin 2018 haar eigen *KodakCoin* lanceerde, steeg de koers van het bedrijf met 60%[16]. Volgens Pal zagen we hetzelfde fenomeen ten tijde van de internetzeepbel[17]. Toch mogen we niet vergeten dat tijdens die zeepbel de fundamenten gelegd werden voor de digitale wereld die we vandaag de dag kennen. Het is dan ook niet raadzaam om de technologie al te snel volledig af te schrijven wegens belangrijke uitdagingen en knelpunten. Bovendien ontstaat geregeld de neiging om het potentieel van technologie op korte termijn te overschatten, maar op langere termijn te onderschatten.
Volgens Gartner, een toonaangevend analisten- en adviesbureau gericht op management, zal blockchain meer dan 3.000 miljard aan waarde aan de economie toevoegen. Dat neemt, aldus Gartner midden 2019, niet weg dat 90% van de blockchainimplementaties die nu gebruikt worden, al in 2021 vervangen zullen moeten worden, door de fragmentering en onvolwassenheid van de technologie[18]. Een ander analistenbureau, McKinsey, is pessimistischer. Ondanks de miljarden die in de technologie geïn-

15 Zie D. Waldo, *The administrative state: A study of the political theory of American public administration*, New York: Ronald Press Co, 1948.

16 S. Liao, 'Kodak announces its own cryptocurrency and watches stock price skyrocket', *The Verge*, 9 januari 2018, www.theverge.com/2018/1/9/16869998/kodak-kodakcoin-blockchain-platform-ethereum-ledger-stock-price.

17 A. Pal, 'Blockchain name-grabbing has echoes of dotcom bubble', *Reuters*, 8 februari 2018, www.reuters.com/article/us-blockchain-companies/blockchain-name-grabbing-has-echoes-of-dotcom-bubble-idUSKBN1FS1F3.

18 *Gartner Predicts 90% of Current Enterprise Blockchain Platform Implementations Will Require Replacement by 2021*, Gartner 3 juni 2019, https://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain.

vesteerd zijn, is het bewijs voor een praktische en schaalbare toepassing van blockchain zeer dungezaaid[19], aldus het analistenbureau. In opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het Ministerie van Justitie en Veiligheid deden enkele onderzoekers van Tilburg University recent een verkennend onderzoek naar de kansen en risico's van blockchaintechnologie vanuit juridisch perspectief.[20] Het rapport is op verschillende vlakken kritisch over de toepassingsmogelijkheden van blockchain door de Nederlandse overheid, maar stelt wel dat als blockchain kansen biedt, deze moeten worden benut.

Alles wat mogelijk is met behulp van een gedistribueerde blockchainbenadering is vanuit een puur technologisch standpunt in beginsel op een efficiëntere en eenvoudigere manier te regelen met een gecentraliseerde benadering. Indien er echter geen geschikte partij is die de rol van centrale vertrouwde partij op zich kan nemen, indien dit praktisch onhaalbaar of onwenselijk is, of te grote risico's inhoudt, is een gedistribueerde benadering te overwegen. Hier ligt volgens ons de meerwaarde van blockchain.
Samengevat is blockchain een gedistribueerde technologie die belooft de afhankelijkheid van intermediaire partijen drastisch te reduceren, maar die vandaag de dag nog in zijn kinderschoenen staat. Het blijft moeilijk of zelfs onmogelijk te voorspellen in welke mate de verwachtingen daadwerkelijk zullen worden waargemaakt.

## 1.3. Wat is blockchain?

> *'The Blockchain is like a book. The pages are numbered. […] The book is published and all people can see it. Since it is stored in many places at the same time and no single place can control all nodes, one will not be able to convince the world of a fake version of the truth.'*[21]
>
> Marc Taverner, (voormalige) Global ambassador and markets developer, Bitfury Group

### 1.3.1. *Peer-to-peer gegevensstructuur*

In essentie is blockchain een gedistribueerde gegevensstructuur – een soort gegevensbank – waar enkel collectief door het peer-to-peer netwerk zonder centrale partij digitaal ondertekende gegevens aan toegevoegd kunnen worden. Deze gegevens moeten

19 M. Higginson, M. Nadeau & K. Rajgopal, *Blockchain's Occam problem*, McKinsey, januari 2019, https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem.

20 M. Schellekens, T.F.E. Tjong Tjin Tai, W. Kaufmann, F. Schemkes & R. Leenes, *Blockchain en het recht. Een verkenning van de reguleringsbehoefte*, Tilburg Universiteit, juni 2019, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/08/28/tk-bijlage-blockchain-en-het-recht-def/tk-bijlage-blockchain-en-het-recht-def.pdf.

21 Zie voor citaat: M. Nimfuehr, 'Blockchain application land register: Georgia and Sweden leading', *Medium*, 3 december 2017, https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa9800170c.

aan bepaalde voorwaarden (regels) voldoen, wat eveneens collectief geverifieerd wordt. Aan de Bitcoin-blockchain kunnen we bijvoorbeeld transactiegegevens toevoegen die, vereenvoudigd, een dergelijke boodschap bevatten: '*Ik, Bob, wil een halve bitcoin transfereren naar Alice*'. Het netwerk verifieert collectief of de ondertekenaar van de transactie, Bob, over voldoende onuitgegeven bitcoins beschikt en, indien dit zo is, wordt de transactie door het netwerk aanvaard door haar aan de blockchain toe te voegen. De blockchain bevat dus de volledige geschiedenis van alle transacties. Daaruit kan afgeleid worden hoeveel bitcoins iedereen bezit.

In de blockchainwereld wordt een set van gegevens die digitaal ondertekend zijn, steeds een *transactie* genoemd, al hoeft er niet per se sprake te zijn van een transfer van waarde. Het kan ook om een loutere registratie gaan, zoals de registratie van een testament of de registratie dat een bepaald document ontvangen is (cfr. aangetekende zending).

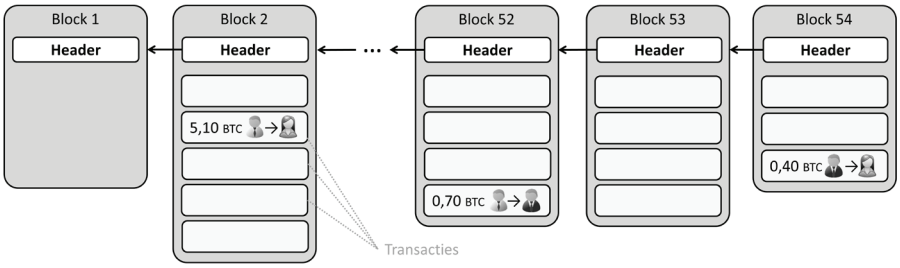
Die transacties worden gegroepeerd in blokken die met een bepaalde frequentie collectief door het netwerk achteraan de blockchain toegevoegd worden. 'Blockchain' is dus een keten (*chain*) van blokken (*blocks*). Bij Bitcoin is de streeffrequentie bijvoorbeeld één blok per tien minuten. Het laatste blok bevat bijgevolg de meest recent verwerkte transacties. De blockchain bevat dus alle verwerkte transacties, van de allereerste tot de allerlaatste. Vanaf de opname in de blockchain – of eventueel een korte tijd later – zijn de transacties in beginsel onwijzigbaar en niet-verwijderbaar. Vele participanten in het blockchainnetwerk bezitten een lokale kopie van de blockchain die ze up-to-date houden. We noemen hen *nodes*. Iedereen heeft dus dezelfde versie van de blockchain. De technologie kan hierdoor gebruikt worden voor het uitwisselen van gegevens en waarde, terwijl gegarandeerd wordt dat iedereen over dezelfde en meest actuele informatie daarover beschikt. Elk blok bevat bovendien een tijdstempel die door het netwerk collectief gevalideerd is.[22] We weten dus exact wanneer een transactie in de blockchain opgenomen werd. Antedatering wordt zo uitgesloten.

Een blockchain is dus een steeds groeiende sequentiële gegevensstructuur, zoals geïllustreerd in figuur 1, die door verschillende partijen in het netwerk bewaard wordt en zo veilig gehouden wordt. Ze bevat de volledige transactiegeschiedenis van de toepassing of toepassingen die ervan gebruikmaken. Dergelijk *append-only*-mechanisme betekent dat alleen blokken kunnen worden toegevoegd aan een blockchain, maar nooit kunnen worden verwijderd[23]. Het aanpassen van gegevens in een blockchain kan niet door aanpassing van bestaande blokken, maar enkel door toevoeging van een nieuw blok met de gewijzigde informatie. Elk blok heeft een *header* die diverse informatie bevat, onder meer een tijdstempel en de hash van het vorige blok. Die hash is – enigszins vereenvoudigd – een soort unieke *fingerprint* die verwijst naar het vorige blok. Zo ontstaat een ketting, een *chain*, van *blocks*, een blockchain dus.

22 Zie A. Schram, 'De bewijskracht van de "blockchain timestamp" in auteursrechtelijke geschillen', *NJB* 2019/2779, afl. 44.

23 V.I. Laan & A. Rutjes, 'Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?', *Computerrecht* 2017/253, 1.

Het telkens opnieuw doorlopen van deze sequentiële structuur door de validerende participanten, om na te gaan of een bepaalde actie of transactie aan de regels voldoet, zou bijzonder inefficiënt zijn. Daarom bewaren deze participanten afzonderlijk, in een efficiënte gegevensbank, de gegevens die relevant zijn voor het valideren van de regels, wat kan worden afgeleid uit de blockchain. Zo staat bijvoorbeeld de volledige Bitcoin-*geschiedenis* op de blockchain, maar de *actuele status* – wie beschikt nu over welke bitcoins – wordt apart bewaard. Enkel dit laatste is immers nodig om na te gaan of iemand het recht heeft bepaalde bitcoins uit te geven.




Figuur 1. Illustratie van de Bitcoin-blockchain. Voor drie transacties geven we een zicht op de inhoud, namelijk het transfereren van bitcoins.

### 1.3.2. *Cryptografie*

Blockchain maakt intensief gebruik van *cryptografie*. Dit is het gebruik van wiskundige principes om gegevens te beschermen. Eigenschappen zoals integriteit (onwijzigbaarheid) en confidentialiteit (vertrouwelijkheid) van gegevens kunnen met behulp van cryptografie gegarandeerd worden. Het gebruik van cryptografie impliceert natuurlijk niet automatisch dat alles altijd ook 100% veilig is.

#### A. *Hashing*

Blockchaintechnologie maakt intensief gebruik van cryptografische hashfuncties. Dit laat toe om een unieke digitale vingerafdruk van om het even welke data te berekenen. Je kunt een vingerafdruk berekenen van een gegevensbank die terabytes groot is, maar evengoed een paar woorden of karakters. De lengte van de vingerafdruk is constant, onafhankelijk van de grootte van de invoer (bijvoorbeeld 32 bytes voor het populaire hashing algoritme genaamd '*SHA256*'). De decimale voorstelling van de SHA256-hash van 'Hello world' is bijvoorbeeld:
869913660443924676617831651669733090238071816480247187783135263898928609948 42.
Als we van zowel de 'h' en de 'w' hoofdletters maken, krijgen we 'Hello World', wat resulteert in een totaal andere hash, namelijk:
748889642472929432908296443649544736093427492511115226347542820697252403006 54.

Wanneer de invoer voldoende groot en onvoorspelbaar is, lekt een hash geen informatie daarover. Uit een te kleine invoer of voorspelbare invoer kan wel informatie gehaald worden. Uit de hash van een burgerservicenummer (bsn) kan bijvoorbeeld eenvoudig het oorspronkelijke burgerservicenummer (de invoer) gevonden worden door alle mogelijke getallen die de correcte structuur hebben van een burgerservicenummer – dat zijn er ongeveer 91 miljoen – te hashen. Voor een computer is dit makkelijk. Een andere belangrijke eigenschap van een cryptografische hashfunctie houdt in dat het onhaalbaar is om twee verschillende invoeren te vinden die resulteren in dezelfde hash. Twee verschillende documenten zullen in de praktijk dus steeds een verschillende hash hebben.
Een blok bevat steeds een hash van het voorgaande blok. Stel dat een malafide entiteit erin slaagt een bepaald blok te vervalsen, dan wijzigt ook de hash van het blok en moet dus ook het daaropvolgende blok vervalst worden. Dat blok krijgt daardoor op zijn beurt een nieuwe hashwaarde waardoor ook het blok dat daarop volgt, aangepast moet worden. Samengevat moet de malafide entiteit alle blokken die na het vervalste blok komen, eveneens vervalsen. Dit draagt bij tot de veiligheid van blockchain.

### B. *Pseudoniemen*

Eerder gaven we als voorbeeld een bitcoin-transactie met de volgende boodschap: '*Ik, Bob, wil een halve bitcoin transfereren naar Alice*'. Dit wil echter niet zeggen dat iedereen op het netwerk kan zien dat Bob op een bepaald moment een bepaald bedrag getransfereerd heeft naar Alice. Alice en Bob zijn immers niet gekend op het blockchainnetwerk onder hun echte naam, maar onder een pseudoniem, wat in de blockchainwereld een *adres* genoemd wordt. Iemand met toegang tot de blockchain kan dus bijvoorbeeld wel zien dat pseudoniem A35DS2 beschikt over 5 bitcoins en dat het de dag ervoor rond 16.00 uur een halve bitcoin getransfereerd heeft naar pseudoniem FZR63S, zonder evenwel te weten dat pseudoniemen A35DS2 en FZR63S eigendom zijn van respectievelijk Bob en Alice.
Bij een pseudoniem hoort een geheime private cryptografische sleutel (*private key*), eigenlijk een lang wachtwoord (zie figuur 2). Om een bitcoin-transactie te creëren waarbij je geld vanaf een bepaald pseudoniem transfereert, heb je de bijhorende private sleutel nodig. Daarmee wordt de transactie digitaal ondertekend en bewijs je dat je de eigenaar bent van het pseudoniem. Dit bewijs kan vervolgens door iedereen geverifieerd worden. De geheime private cryptografische sleutel wordt daarbij niet prijsgegeven.


Figuur 2. Een paper wallet (papieren portefeuille) voor Bitcoin, met daarop het publieke adres (pseudoniem) waaronder je bekend bent op het blockchainnetwerk en de private sleutel (private address) die geheim moet blijven.

Digitale handtekeningen zijn een toepassing van asymmetrische cryptografie, wat ook wel publieke sleutelcryptografie genoemd wordt. Dit impliceert dat er gebruikgemaakt wordt van twee gerelateerde sleutels: een private sleutel en een publieke sleutel. Een voorbeeld van een private sleutel zien we links in figuur 2. Het pseudoniem ernaast is de hash van de bijhorende publieke sleutel. Elke transactie bevat zowel een digitale handtekening van de inhoud als de publieke sleutel. Iedereen kan dus met behulp van de publieke sleutel nagaan of de digitale handtekening van de transactie geldig is en dat de ondertekenaar eigenaar is van het pseudoniem.

## 1.4. Public vs. private en permissionless vs. permissioned

Er bestaan verschillende soorten blockchains. Vooreerst is er een verschil mogelijk met betrekking tot de toegang tot een blockchain. Bij een *public* blockchain heeft iedereen toegang. De hele wereld kan dus de blockchain inspecteren. Bij een *private* blockchain daarentegen is toegang beperkt tot een bepaalde groep die is uitgenodigd of die voldoet aan bepaalde voorwaarden[24]. Meestal bepaalt een centrale verwerker wie toegelaten wordt. Er wordt tevens een onderscheid gemaakt tussen *permissionless* en *permissioned* blockchainnetwerken[25].

*Permissionless* bockchainnetwerken zijn netwerken waarin iedereen die toegang heeft tot de blockchain er ook naar eigen goeddunken in kan participeren en – in theorie althans – gelijke rechten heeft. In de praktijk zijn dit vaak publieke, open netwerken. Voorbeelden zijn Bitcoin, Ethereum en Litecoin. Iedereen met een internetverbinding heeft toegang tot de volledige blockchain, wat leidt tot transparantie, en iedereen kan volwaardig participeren in het netwerk, bijvoorbeeld via het creëren en het publiceren

24 *Ibid.*, 5.

25 A. Kadiyala, 'Nuances Between Permissionless and Permissioned Blockchains', *Medium*, 18 februari 2018, https://medium.com/@akadiyala/nuances-between-permissionless-and-permissioned-blockchains-f5b-566f5d483.

van transacties of het meeparticiperen in het collectief veilig houden van de blockchain. Er is een systeem van incentives (stimulansen) om alles correct te laten verlopen. Om gebruik te maken van het netwerk zul je in beginsel virtueel geld moeten betalen. Draag je bij aan het veilig houden van het netwerk, dan kun je virtueel geld verdienen. Dergelijke blockchainnetwerken kunnen wereldwijd uit vele duizenden participanten bestaan. Door het open karakter kun je een *permissionless* blockchainnetwerk vergelijken met internet. Vandaag de dag gebruiken de voornaamste *permissionless* blockchainnetwerken *Proof of Work* (doorgaans afgekort als '*PoW*') als consensusmechanisme, wat garandeert dat iedereen met dezelfde versie van de blockchain werkt (*infra* 1.5. Consensusmechanisme). PoW heeft echter als nadeel dat het enorm veel energie verbruikt (*infra* 3.5. Ecologische impact).

In tegenstelling tot *permissionless* blockchainnetwerken waarbij alle gebruikers gelijkwaardig zijn en dezelfde rechten hebben, is dit niet het geval bij *permissioned* blockchainnetwerken. Rond het netwerk bevindt zich dan niet alleen een toegangscontrolelaag die bepaalt wie toegang heeft tot het blockchainnetwerk, maar vooral ook wie wat mag doen. Hierdoor is er geen sprake meer van een volledig gedistribueerd netwerk. Zo kan het zijn dat Alice wel transacties kan plaatsen, maar niet instaat voor het veilig en operationeel houden van de blockchain. Dat wordt overgelaten aan Bob en anderen bijvoorbeeld. In een dergelijk netwerk kennen de partijen elkaar of is er op zijn minst een manier om participanten te identificeren. Dergelijke netwerken hebben doorgaans veel minder participanten en kun je vergelijken met een intranet, een afgeschermde internetachtige omgeving van een bedrijf of consortium. *Permissioned* blockchainnetwerken zijn doorgaans een stuk energie-efficiënter en sneller dan de *permissionless* netwerken. Enerzijds zijn er immers minder partijen betrokken in de validatie, waardoor de graad waarin het vertrouwen is gedistribueerd lager is dan bij *permissionless* netwerken. Anderzijds laten *permissioned* blockchainnetwerken meer transacties per seconde toe en worden deze sneller verwerkt.

In de praktijk zijn publieke blockchains momenteel vaak *permissionless* en private blockchains *permissioned*. Volgens sommigen staan *permissioned* blockchains echter haaks op de onderliggende filosofie van blockchain, aangezien openheid, transparantie en pseudonimiteit worden opgegeven en er eerder sprake is van een toepassing die gedecentraliseerd is in plaats van gedistribueerd. In een gedecentraliseerde toepassing staat slechts een beperkt aantal entiteiten in voor het aanbieden van de dienst, terwijl in een gedistribueerde toepassing elke gebruiker de mogelijkheid heeft daaraan bij te dragen.

Er bestaan ook hybride oplossingen. Een voorbeeld is *Ripple*. Iedereen kan Ripple gebruiken voor financiële transacties, maar het verwerken van die transactie in de blockchain en het veilig houden ervan is het werk van een beperkt aantal vaste validatoren. Vertrouwen is dus minder gedistribueerd, maar je wint wel aan verwerkingscapaciteit. Ripple is in staat 1.500 transacties per seconde te verwerken, met een gemiddelde verwerkingssnelheid van drie tot vijf seconden. Dat is heel wat anders dan Bitcoin dat minder dan tien transacties per seconde aankan en waarbij ongeveer een uur gewacht moet worden vooraleer een transactie als definitief aanvaard beschouwd kan worden.

De *Libra*, de virtuele munt die Facebook wil lanceren, zal eveneens gebruikmaken van een *permissioned* blockchain. Het zal immers veilig gehouden worden door – op het moment van schrijven – eenentwintig bedrijven. Het is op het moment van schrijven wel nog onduidelijk of het ook publiek zal zijn, of, met andere woorden, anderen de blockchain zullen kunnen inspecteren. Het is bovendien onzeker of de Libra – sowieso een gedurfd project – er ooit wel zal komen[26].

## 1.5. Consensusmechanisme

Het *consensusmechanisme* zorgt ervoor dat elke participant in het netwerk die een kopie van de blockchain heeft (*i.e. node*) over dezelfde versie beschikt. Een *node* is met meerdere andere *nodes* verbonden en vormt zo dus een knooppunt in het netwerk.
In *permissionless* blockchainnetwerken is vandaag de dag vooral PoW (*Proof of Work*) populair. Onder meer Bitcoin en Ethereum maken hier gebruik van. PoW houdt in dat er een permanente competitie is tussen een (klein) deel van de participanten – de *miners* of delvers – om als eerste een nieuw blok te creëren. Daartoe moet een soort puzzel gevonden worden wat veel moeite (rekenkracht) kost. Wanneer een participant daarin slaagt, stuurt hij het blok zo snel mogelijk naar de participanten waarmee deze verbonden is. De andere participanten gaan vervolgens na of alles in orde is met het blok en de transacties erin, mede op basis van de eigen, lokale blockchainkopie. Enkel indien dit het geval is, wordt het blok toegevoegd aan die lokale blockchainkopie en verder doorgestuurd op het netwerk. De participanten die het vervolgens ontvangen, doen hetzelfde. Deze propagatie van het nieuwe blok gaat zo verder tot, na maximaal een paar seconden, het hele blockchainnetwerk het nieuwe blok ontvangen en gevalideerd heeft.
Vanaf het moment dat een delver een nieuw blok gecreëerd heeft, begint de competitie voor het volgende blok. De winnende delver krijgt een beloning in de vorm van nieuw gecreëerd virtueel geld en/of transactievergoedingen. Vanaf het moment dat een transactie is opgenomen in de blockchain, kan deze in beginsel niet meer verwijderd of gewijzigd worden. Hoe langer de transactie zich erin bevindt, hoe sterker deze bovendien in de blockchain gebetonneerd is.
Er zijn verschillende types PoW. Ethereum en Bitcoin bijvoorbeeld maken gebruik van totaal verschillende types PoW (voor het Bitcoin PoW consensusmechanisme, *infra* 3.5. Ecologische impact). Er zijn echter ook alternatieven, zoals *Proof of Stake* (PoS)[27] die aan populariteit winnen. Een participant zet daarbij een deel van zijn virtuele munten in. Als zijn deel x% van de totale inzet bedraagt, zal de participant ook x% van de blokken creëren. Indien hij valsspeelt, verlies hij zijn inzet. Als hij het spel eerlijk speelt, ontvangt hij een beloning, meestal in de vorm van transactievergoedingen. Dit consen-

26 L. Dodds, 'How Facebook's vision for Libra turned into a nightmare', *The Telegraph*, 3 januari 2020. https://www.telegraph.co.uk/technology/2020/01/03/facebooks-vision-libra-turned-nightmare/.
27 S. Ray, 'What is Proof of Stake?', *Hackernoon*, 6 oktober 2017, https://hackernoon.com/what-is-proof-of-stake-8e0433018256.

susmechanisme is veel energie-efficiënter, maar controversieel[28]. Ethereum, het bekendste blockchaingebaseerde smartcontractplatform, is al een tijdje van plan over te schakelen op PoS.
Er zijn ondertussen ook verschillende virtuele munten, zoals *TRON* en *EOS,* gebaseerd op *Delegated Proof of Stake* (DPoS), waarbij een beperkte groep verkozen wordt om het netwerk veilig te houden. Ook dit is veel energie-efficiënter dan PoW. Doordat een kleinere groep instaat voor het veilig houden van de blockchain, is er een hogere verwerkingscapaciteit (aantal transacties per seconde) mogelijk.
*Permissioned* blockchainnetwerken maken gebruik van andere principes. Een aantal participanten in het netwerk krijgt het recht om collectief transacties te valideren en/of in de blockchain te verwerken. Dit kan op het niveau van de blockchain zijn (*proof of authority*), maar eventueel ook op het niveau van een specifiek smart contract op die blockchain. Verschillende participanten kunnen een verschillend gewicht krijgen bij het valideren van transacties. Een transactie is gevalideerd vanaf het moment dat een vastgelegd quorum bereikt wordt.

## 1.6. Staat van de technologie

Hoewel de technologie als veelbelovend wordt gezien, zal het nog verschillende jaren duren vooraleer ze volwassen is. Dit impliceert dat het vandaag de dag meestal veel inspanning vergt, geld kost en ook risico's inhoudt om blockchaintoepassingen operationeel te maken en te houden. Bedrijven of overheden die nu al op blockchain gebaseerde toepassingen in bedrijf hebben, beperken daarom doorgaans hun ambities. Ze maken gebruik van de eenvoudige mogelijkheden die de technologie biedt, en gebruik van de technologie in meer uitdagendere toepassingen wordt doorgaans vermeden.
Toch houdt dit bedrijven en overheden niet tegen om al volop met de technologie te experimenteren. In een eerste fase werden vooral veel *Proof of Concepts* (softwareprototypes) (PoC) ontwikkeld, die weliswaar de mogelijkheden van de technologie illustreren, maar waar doorgaans verder niet veel meer mee gebeurt. Dit was deels te verklaren door de onvolwassenheid van de technologie. De technologie was natuurlijk ook enorm *gehypet* en velen voelden de drang om sneller dan de concurrentie iets te kunnen aankondigen of vreesden om uit de boot te vallen. Dit laatste wordt ook wel *FOMO*, ofwel *Fear of Missing Out*, genoemd. Bij het maken van een PoC werden vragen zoals '*Hebben we daar echt een blockchain voor nodig?*', '*Zijn de veiligheid en privacy voldoende sterk gegarandeerd?*', '*Is het geheel voldoende schaalbaar?*', '*Wat kost het om dit alles operationeel te brengen en te houden?*' en '*Is alles juridisch in orde?*' niet steeds afdoende beantwoord, waardoor het natuurlijk moeilijk wordt om de volgende stap te zetten nadat het PoC voltooid is.
Geleidelijk aan gaan bedrijven en overheden wel verder dan de '*PoC-only*'-fase. Een aantal beloftevolle toepassingen zoals We.Trade en VAKT, waar ook Nederlandse be-

28 A. Sharma, 'Understanding Proof of Stake through it's Flaws', *Medium*, 15 januari 2018, https://medium.com/@abhisharm/understanding-proof-of-stake-through-its-flaws-pt-1-6728020994a1.

drijven in participeren, worden al in de praktijk gebruikt (*infra* hoofdstuk 5, Blockchain smart).
Blockchaintechnologie laat toe om afhankelijkheid van autoriteiten te reduceren. De prijs die je ervoor betaalt, is transparantie. Meerdere entiteiten in het netwerk moeten immers in staat zijn om bepaalde validaties te doen vooraleer iets in de blockchain geregistreerd wordt. Hoe rijm je dit vervolgens met privacy en confidentialiteit van gevoelige gegevens en dus de bescherming van persoonsgegevens? Daarnaast zijn er fundamentele beperkingen wat betreft schaalbaarheid of verwerkingscapaciteit (*i.e.* het aantal transacties dat per seconde door het netwerk verwerkt kan worden). Hoofdstuk 7, Blockchain en gedistribueerd vertrouwen gaat hier dieper op in. Er ontstaat dus een trilemma (*infra* 7.5. Het blockchaintrilemma), namelijk een spanningsveld tussen distributie van vertrouwen, veiligheid en schaalbaarheid. Als we één van deze drie aspecten verbeteren, gaat dit ten koste van minstens één van de andere aspecten. We moeten evenwel indachtig houden dat blockchain vaak slechts één component is van een praktijktoepassing. Doorgaans zijn nog allerlei additionele componenten naast de blockchain nodig om een toepassing daadwerkelijk te operationaliseren.
De stelling dat het elimineren van een vertrouwde autoriteit in een proces dat proces automatisch efficiënter en goedkoper maakt, blijkt niet steeds te kloppen. We zullen bijvoorbeeld aantonen dat een bitcoin-transactie niet steeds goedkoper is dan een traditionele financiële transactie. Bovendien kunnen het opzetten en het onderhouden van een afgeschermd blockchainnetwerk tussen verschillende partijen duurder zijn dan het opzetten en het onderhouden van een centrale server (*infra* 7.3. Kostprijs van gedistribueerd vertrouwen).
Er geldt dus nog steeds: '*There is no such thing as a free distributed lunch*'. Toch betekent dit geenszins dat de technologie al te snel afgeschreven moet worden. Ook op dit moment kan ze al nuttig ingezet worden. Naarmate de technologie volwassener wordt, zal ook het gebruik ervan makkelijker en goedkoper worden en zal ze ingezet kunnen worden voor meer grootschalige en uitdagende toepassingen. Hoewel alle uitdagingen binnen een paar jaar niet volledig opgelost zullen zijn, zal de toestand van de technologie in de toekomst verder staan dan vandaag, met de aangehaalde beperkingen.

## 1.7. (Nood aan) juridisch kader

Er zal telkens moeten worden nagegaan welke sectorspecifieke, materiële wetgeving in het betreffende rechtsdomein van toepassing is, afhankelijk van de sector waarin blockchain toegepast wordt. Dat heeft ook een impact op welke toezichthouders mogelijk een rol spelen, zowel op nationaal als op Europees vlak. In elk geval zal al in de ontwerpfase van de blockchain ('*by design*') bij elke blockchaintoepassing telkens voldoende aandacht moeten gaan naar de conformiteit met de privacywetgeving en dan vooral de Algemene Verordening Gegevensbescherming die op 25 mei 2018 in werking is getreden (*infra* hoofdstuk 6, Privacywetgeving). Belangrijke principes van de AVG, zoals een behoorlijke en rechtmatige verwerking van persoonsgegevens, het recht op rectificatie en vergetelheid, het recht op beperking van de verwerking en pas-

sende beveiliging, stellen blockchainprojecten immers vaak voor grote uitdagingen. Gegevens die worden toegevoegd aan de blockchain, zijn immers in beginsel niet wijzigbaar noch verwijderbaar, wat ook net tegelijkertijd de grootste troef is van blockchaintoepassingen. Hier is duidelijk sprake van een paradox. In elk geval kan *non-compliance* met de AVG soms alleen vermeden worden door geen persoonsgegevens in de blockchain op te nemen, maar deze buiten de blockchain op te slaan of deze te anonimiseren of pseudonimiseren vooraleer ze worden opgenomen[29].

Blockchain maakt meestal gebruik van smart contracts voor het collectief afdwingen van bepaalde regels. Hoewel een 'smart contract' niet per se een juridische overeenkomst hoeft te zijn, kan er wel sprake zijn van het sluiten van een overeenkomst of uitvoeren van verbintenissen uit een overeenkomst (*infra* hoofdstuk 2, Smart contracts). In dat laatste geval is in Nederland in beginsel het verbintenissenrecht uit het Burgerlijk Wetboek van toepassing.

Bij een aankoop door een consument bijvoorbeeld zijn daarnaast ook specifieke regels voor verkoop aan consumenten en consumentenzaken van toepassing. Die regels vinden we zowel in Europese verordeningen[30] als Nederlandse wetten[31]. De regering heeft vervolgens sommige wetten uitgewerkt in een Algemene Maatregel van Bestuur (AMvB)[32]. AMvB's worden dan weer verder uitgewerkt door ministeries in een ministeriële regeling. De Autoriteit Consument & Markt (ACM) tenslotte vult haar beleidsruimte in met behulp van beleidsregels.

Met betrekking tot aansprakelijkheid zou het nuttig kunnen zijn om op basis van de rol die iemand inneemt in de blockchain de aansprakelijkheid duidelijk af te bakenen, net zoals de rechten en verplichtingen in de AVG ook worden afgebakend op basis van de rol die iemand vervult[33]. Hier zou dus wat ons betreft regelgevend kunnen worden opgetreden.

Bij virtuele valuta zoals bitcoins is een belangrijke juridische vraag of deze *cryptocurrencies* gezien moeten worden als een ruilmiddel, een gekocht goed of een betaalmiddel (*infra* 3.10. Juridische kwalificatie van virtuele valuta). Aangezien bij de handel in virtuele valuta geregeld sprake is van misbruik en fraude, heeft de Europese Unie in april 2018 de Vijfde Anti-witwasrichtlijn goedgekeurd (*infra* 3.13. Overheidsregulering). Lidstaten dienen zowel handelsplatformen van virtuele munten als walletbeheerders onder de toepassing van de AML/CFT-regulering (Anti-Money Laundering/

29 Zie V.I. Laan & A. Rutjes, 'Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?', *Computerrecht* 2017/253.

30 Verordening nr. 2006/2004 van het Europees Parlement en de Raad (samenwerking tussen nationale instanties voor consumentenbescherming); verordening Nr. 1008/2008 van het Europees Parlement en de Raad (gemeenschappelijke regels voor de exploitatie van luchtdiensten); verordening nr. 2018/302 van het Europees Parlement en de Raad (aanpak van ongerechtvaardige geoblocking).

31 Wet handhaving consumentenbescherming en Dienstenwet (verkoop aan consumenten); Elektriciteitswet 1998, Gaswet en Telecommunicatiewet (consumentenzaken).

32 Besluit aanwijzing instanties met een rechtmatig belang; Besluit bel-me-niet-register; Besluit elektronische handtekeningen; Besluit universele dienstverlening en eindgebruikersbelangen; Besluit leveringszekerheid Elektriciteitswet 1998; Besluit leveringszekerheid Gaswet; Besluit vergunning levering elektriciteit aan kleinverbruikers; Besluit vergunning levering gas aan kleinverbruikers.

33 E. Valgaeren & J.J. Linnemann, 'Inleiding – Blockchain ontketend', *Computerrecht* 2017/250, p. 3-4.

Combating the Financing of Terrorism) te brengen. Tegen 10 januari 2020 moesten de lidstaten wetgeving aannemen om handelsplatformen en walletaanbieders te registreren. Het is de bedoeling dat hun klanten geïdentificeerd zullen kunnen worden en handelsplatformen verplicht worden verdachte activiteiten te melden. Er is dus sprake van een belangrijke, doch slechts eerste stap om transparantie te brengen in de netwerken van virtuele munten.

In Nederland is op het moment van schrijven (februari 2020) de uitvoering van de richtlijn in het voorstel Implementatiewet wijziging vierde anti-witwasrichtlijn echter nog steeds in behandeling bij de Eerste Kamer. Het wetsvoorstel bevat voornamelijk wijzigingen van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Met dit wetsvoorstel dienen aanbieders van diensten voor het wisselen tussen virtuele valuta en fiat valuta en aanbieders van bewaarportemonnees zich te registreren bij De Nederlandsche Bank (het voorstel van een vergunningenstelsel is ondertussen verlaten) en worden ze onder de reikwijdte van de Wwft gebracht waarvan ze de algemene vereisten dus moeten naleven. Dat betekent onder andere dat zij onderzoek moeten doen naar hun cliënten en ongebruikelijke transacties dienen te melden bij de Financiële Inlichtingen Eenheid (FIU). Aangezien de parlementaire behandeling meer tijd in beslag neemt, geldt de registratieplicht en het vereiste tot naleving van de algemene vereisten van de Wwft dus nog niet vanaf 10 januari 2020.

ICO's (*infra* 3.14. Initial Coin Offerings) op hun beurt waren in het begin overal ter wereld ook geheel ongereguleerd en werden daarom beschouwd als een gemakkelijke manier om ongereguleerd investeringen aan te trekken. We zien nu in verschillende landen echter specifieke regelgeving ontstaan. In Nederland en in de EU werd vooralsnog geen specifieke regelgeving aangenomen. Bij een ICO moet evenwel steeds worden stilgestaan bij de mogelijke toepasselijkheid van EU-regelgeving en de Wet op het financieel toezicht.

De EU heeft nog geen specifieke blockchainregelgeving aangenomen, maar de Europese Commissie heeft wel een *EU Blockchain Observatory and Forum* opgericht[34]. Dit forum ging op 1 februari 2018 officieel van start en brengt onder meer bestaande initiatieven in kaart om zo beter zicht te krijgen op de acties die nodig zijn vanuit de EU. Er is, enerzijds, een *Blockchain Policy and Framework Conditions Working Group* die over verschillende technologieën en industrieën heen de voorwaarden wil detecteren op beleids-, wettelijk en regelgevend vlak die noodzakelijk zijn om de rechtszekerheid te verkrijgen die vereist is om de toepassing op grote schaal van blockchainapplicaties mogelijk te maken. Anderzijds, analyseert de *Use Cases and Transition Scenarios Working Group* de meest veelbelovende, innoverende toepassingen met de nadruk op toepassingen binnen de overheidssector, zoals identiteit, overheidsdiensten, gezondheidszorg, energie en milieurapportage.[35] In verschillende staten van de VS bijvoorbeeld werd al specifieke blockchainwetgeving aangenomen[36].

34 https://ec.europa.eu/digital-single-market/en/eu-blockchain-observatory-and-forum.

35 Zie M. Pomp & R. Verhaert, *Blockchain in de praktijk. Meer dan 50 use cases van de overheid in Nederland en België*, Sdu, 2018.

36 E. Valgaeren & J.J. Linnemann, 'Inleiding – Blockchain ontketend', *Computerrecht* 2017/250, p. 2.

Naast de bijzonder relevante analyse die bestaande wet- en regelgeving mogelijkerwijs van toepassing is op blockchaintoepassingen en dus misschien een hinderpaal kan zijn bij de ontwikkeling van concrete blockchaintoepassingen, zullen beleidsmakers, wetgevingsjuristen en academici – in nauw overleg met technische specialisten – ook moeten nadenken over nieuwe wetgevende kaders. Indien blockchain immers nog maar een gedeelte realiseert van wat het belooft, zal de impact ontegensprekelijk immens zijn. We hebben in dit opzicht echter nood aan doordachte wetgeving die toekomstbestendig is in een domein waar de snelheid van technologische evoluties alleen maar zal toenemen. Zo is blockchain slechts één mogelijke vorm, doch momenteel de meest populaire, van *Distributed Ledger Technology* (DLT) die leidt tot hyperconnectiviteit. DLT maakt gebruik van een datastructuur waar gegevens aan toegevoegd kunnen worden (het digitale grootboek, de *ledger*) die collectief gedeeld en veilig gehouden wordt. In de financiële sector en in de verzekeringssector zouden blockchain en smart contracts aanzienlijke efficiëntiewinsten kunnen opleveren. De bestaande regelgeving in deze sectoren is echter vooral gericht op tussenpersonen, waardoor nieuwe gedecentraliseerde technologie zoals blockchain een nieuw regelgevend kader lijkt te vereisen[37].

Het principe van functionele equivalentie, zoals bijvoorbeeld ingebed in artikel 9.1 Richtlijn elektronische handel[38], zou als een goede inspiratiebron kunnen dienen bij nieuwe wetgevende initiatieven[39]. Volgens de theorie van de functionele equivalentie moeten we ons niet blindstaren op het gekozen middel maar moeten we kijken naar de achterliggende doelstelling om te bepalen of aan wettelijke of reglementaire vormvereisten is voldaan. Zo kan 'elektronisch' bij elektronisch handelsverkeer bijvoorbeeld vaak als functioneel equivalent worden beschouwd van 'schriftelijk'[40]. Ook bij blockchain of andere *distributed ledger* technologieën zou een dergelijke aanpak voor meer rechtszekerheid kunnen zorgen.

Het lijkt ons raadzaam om bij de vormgeving van nieuwe wet- en regelgeving toekomstbestendig op te treden en ook al verder te kijken dan blockchain (*infra* 7.6. Beyond blockchain). In het ICT-recht werden we al overspoeld met nieuwe wetgeving. Daarnaast komen nieuwe wetgevende initiatieven uit verschillende domeinen, terwijl een goede coördinatie ontbreekt. Dit leidt onder meer tot botsende verplichtingen en uiteenlopende definities, bijvoorbeeld in de verhouding tussen de AVG en het ontwerp

37 A. De Backer & V. De Boe, 'Smart contracts in de financiële sector: grote verwachtingen en regulatoire uitdagingen', *Computerrecht* 2017/252.

38 '*De lidstaten zorgen ervoor dat hun rechtsstelsel het sluiten van contracten langs elektronische weg mogelijk maakt. Zij vergewissen zich er met name van dat de regels met betrekking tot de totstandkoming van contracten geen belemmering vormen voor het gebruik van langs elektronische weg gesloten contracten, noch ertoe leiden dat dergelijke contracten, omdat zij langs elektronische weg tot stand zijn gekomen, zonder rechtsgevolg blijven en niet rechtsgeldig zijn*', Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, *Pb.L.* 17 juli 2000, afl. 178.

39 E. Valgaeren & J.J. Linnemann, 'Inleiding – Blockchain ontketend', *Computerrecht* 2017/250, p. 4.

40 A.R. Lodder, 'Elektronisch handelsrecht. De juridische aspecten van elektronische communicatie in het handelsrecht. Proefschrift van mr. H.P.A.J. Martius', *Maandblad voor Vermogensrecht* 2009, nr. 1, 17.

van de E-Privacyverordening[41] die in 2020 wordt verwacht als aanvulling op de AVG, of de AVG en de Netwerk- en Informatiebeveiligingsrichtlijn[42, 43]. Een gecoördineerde, toekomstbestendige aanpak is dus nodig. Hoewel aankondigingspolitiek vermeden dient te worden en de wetgever met voldoende kennis van zaken en voldoende zicht op de praktische werking en implicaties aan het werk moet gaan, kan de wetgever het zich niet veroorloven om al te lang een juridisch vacuüm of onzekerheid met betrekking tot toepasselijke regelgeving in stand te houden. Dit staat immers op gespannen voet met het rechtszekerheidsbeginsel en kan in de praktijk een rem betekenen op nieuwe ontwikkelingen die de maatschappij ten goede zouden komen.
Daarnaast stelt de vraag zich naar het geschikte niveau om de juridische (en andere) uitdagingen met betrekking tot blockchain op te vangen. Elk land dient zich te bezinnen over regelgevend ingrijpen en het lijkt overduidelijk dat de EU niet achter kan blijven om tot een geharmoniseerde aanpak te komen. Blockchaintoepassingen overschrijden immers al snel de landsgrenzen en blijven geregeld ook niet binnen het EU-grondgebied. Een mondiale dialoog en internationale afspraken lijken dus geen overbodige luxe in een blockchainwereld.

## 1.8. Toepasselijk recht

Zoals hiervoor aangegeven, zal telkens moeten worden nagegaan welke sectorspecifieke, materiële wetgeving in het betreffende rechtsdomein van toepassing is. Dit is afhankelijk van het domein waarin blockchain toegepast wordt, bijvoorbeeld virtuele valuta, vastgoedtransacties, de zorg- of energiesector. Daarnaast moet rekening worden gehouden met de privacywetgeving bij de verwerking van persoonsgegevens en dan vooral de AVG (*infra* hoofdstuk 6, Privacywetgeving).
Hoewel een 'smart contract' niet per se een juridische overeenkomst is, is er wel vaak sprake van het sluiten van een overeenkomst of uitvoeren van verbintenissen uit een overeenkomst (*infra* hoofdstuk 2, Smart contracts). Om te bepalen wat het toepasselijke recht is, moet voor elk mogelijk toepasselijk rechtsgebied worden nagegaan wat de toepassingsvoorwaarden zijn[44]. Aangezien blockchain geregeld de landsgrenzen overschrijdt, is het ook zeker niet ondenkbaar dat regelgeving uit verschillende rechtsordes

41 Voorstel (Comm.) voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie), 10 januari 2017, COM(2017) 10 final – 2017/0003 (COD).

42 Richtlijn 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, *Pb.L.* 19 juli 2016, afl. 194, 1. Zie J.P. Kalis, 'De Netwerk en Informatiebeveiligingsrichtlijn', *Computerrecht* 2017/48, p. 61.

43 E. Valgaeren & J.J. Linneman, 'Inleiding – Blockchain ontketend', *Computerrecht* 2017/250, p. 3.

44 Zie S. Van Heukelom, J. Naves & M. Van Graafeiland, 'Whitepaper. Juridische aspecten van blockchain', *Pels Rijcken*, 4, www.pelsrijcken.nl/actueel/publicaties/whitepaper-juridische-aspecten-van-blockchain. Zie ook H. Schuringa, 'Enkele civielrechtelijke aspecten van blockchain', *Computerrecht* 2017/254; M. Schellekens, T.F.E. Tjong Tjin Tai, W. Kaufmann, F. Schemkes & R. Leenes, *Blockchain en het recht. Een verkenning van de reguleringsbehoefte*, Tilburg Universiteit, juni 2019, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/08/28/tk-bijlage-blockchain-en-het-recht-def/tk-bijlage-blockchain-en-het-recht-def.pdf, par. 3.2.12.

van toepassing is, bijvoorbeeld het verbintenissenrecht uit land A en het fiscaal recht uit land B.

Indien personen uit meerdere landen betrokken zijn, zullen voor het burgerlijk recht de regels van het internationaal privaatrecht moeten worden toegepast om te bepalen welk nationaal recht van toepassing is, tenzij de betrokken partijen uitdrukkelijk zelf een keuze hebben gemaakt[45]. Bij gebrek aan uitdrukkelijke keuze, zal het telkens van belang zijn om de betrokken rechtshandeling goed juridisch te kwalificeren, de nationaliteit van de betrokken actoren te bepalen (wat moeilijk kan zijn in publieke blockchains waar gebruik wordt gemaakt van pseudoniemen) en welke internationale afspraken of regels mogelijk van toepassing zijn[46]. De uitdrukkelijke keuze van de partijen is in beginsel ook leidend om de bevoegde rechter te bepalen[47]. Voor de rechterlijke bevoegdheid met betrekking tot burgerlijke en handelszaken is het relevant om te wijzen op de toepasselijkheid van de EEX-Verordening indien partijen uit verschillende EU-landen komen[48].

Bij een transactie tussen twee Nederlanders via blockchain is in beginsel – tenzij andersluidend contractueel beding – het verbintenissenrecht uit het Burgerlijk Wetboek van toepassing. Wanneer partijen uit verschillende EU-lidstaten zijn betrokken en uit het recht van verschillende landen moet worden gekozen, moet worden gekeken naar de Rome I-Verordening met betrekking tot het recht dat van toepassing is op verbintenissen uit overeenkomst.[49] Deze verordening is alleen van toepassing op verbintenissen uit overeenkomst in burgerlijke en handelszaken, en niet op fiscale, administratiefrechtelijke en douanezaken[50]. Het recht aangewezen door de verordening is toepasselijk ongeacht de vraag of het gaat om het recht van een EU-lidstaat[51]. Het leidende principe is de rechtskeuze door de partijen. De – gehele of een deel van de – overeenkomst wordt dus beheerst door het recht dat de contracterende partijen hebben gekozen. Deze rechtskeuze is ofwel expliciet, ofwel blijkt duidelijk uit de bepalingen van de overeenkomst of uit de omstandigheden van het geval[52].

Bij gebrek aan rechtskeuze door de partijen is in beginsel het recht van toepassing van het land waar de partij die de *kenmerkende prestatie* van de overeenkomst moet verrichten, zijn of haar gewone verblijfplaats heeft, tenzij uit de omstandigheden blijkt dat de overeenkomst een kennelijk nauwere band heeft met een ander land[53].

45 Smart Contract Working Group – Dutch Blockchain Coalition, *Smart contracts as a specific application of blockchain technology*, 36, https://dutchblockchaincoalition.org/uploads/pdf/Smart-Contracts-ENG-report.pdf.

46 *Ibid.*, 36-37.

47 *Ibid.*, 37.

48 Verordening nr. 1215/2012 van het Europees Parlement en de Raad van 12 december 2012 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken, *Pb.L.* 20 december 2012, afl. 351, 1.

49 Verordening nr. 593/2008 van het Europees Parlement en de Raad van 17 juni 2008 inzake het recht dat van toepassing is op verbintenissen uit overeenkomst, *Pb.L.* 4 juli 2008, afl. 177, 6 (Rome I-Verordening).

50 Art. 1 Rome I-Verordening.

51 Art. 2 Rome I-Verordening.

52 Art. 3 Rome I-Verordening.

53 Art. 4, leden 2 en 3 Rome I-Verordening.

Stel: een Nederlander koopt via internet een tweedehandsauto van een Duitser, waarbij beiden natuurlijke personen zijn die niet handelen in de uitoefening van hun bedrijf of beroep. De Nederlander koopt de auto met de cryptocurrency bitcoin waardoor deze transactie op de blockchain plaatsvindt. De levering van de auto is hier de kenmerkende prestatie die de transactie onderscheidt van andere transacties (niet de betaling)[54]. De overeenkomst en dus de transactie van de auto en de bitcoins worden, bij gebrek aan rechtskeuze door de partijen, beheerst door het Duitse civiele recht.
Voor sommige soorten overeenkomsten bepaalt de Rome I-Verordening uitdrukkelijk welk recht van toepassing is; deze regels leggen in feite vast welk land in zulke gevallen de nauwste band heeft.[55]
Voor verbintenissen uit onrechtmatige daad geldt op basis van de Rome II-Verordening het recht van het land waar de schade zich voordeed.[56] Indien partijen echter beide uit hetzelfde land komen, of een ander land een nauwere band heeft, is het recht uit dat land van toepassing.[57] Voor niet-EU-gevallen waarop wel het Nederlandse IPR van toepassing is, bevatten de artikelen 10:153-10:159 BW in essentie dezelfde regels als de Rome I- en Rome II-Verordeningen.
De bouwers van een blockchain hebben auteursrechten op de software die ze ontwikkeld hebben, hoewel bij publieke blockchains deze software in beginsel wel *open source* beschikbaar wordt gesteld. In Nederland betekent dit dus toepasselijkheid van de regeling van de Auteurswet van 23 september 1912.

54 Zie S. Van Heukelom, J. Naves & M. Van Graafeiland, 'Whitepaper. Juridische aspecten van blockchain', *Pels Rijcken*, 4, www.pelsrijcken.nl/actueel/publicaties/whitepaper-juridische-aspecten-van-blockchain.
55 Art. 4, lid 1 t/m art. 6 Rome I-Verordening.
56 Art. 4 lid 1 Verordening 864/2007 van het Europees Parlement en de Raad van 11 juli 2007 betreffende het recht dat van toepassing is op verbintenissen uit onrechtmatige daad, Pb.L. 31 juli 2007, afl. 199, 40 (Rome II-Verordening).
57 Art. 4 lid 2 en 3 Rome II-Verordening.

# 2. Smart contracts

*'A mechanism involving digital assets and two or more parties, where some or all of the parties put assets in and assets are automatically redistributed among those parties according to a formula based on certain data that is not known at the time the contract is initiated'*[58].

Vitalik Buterin, bedenker van het Ethereum-smartcontractplatform

## 2.1. Inleiding

Een blockchainnetwerk dwingt collectief bepaalde regels af. In het geval van virtuele munten is de voornaamste regel: '*Je kunt enkel eigen, onuitgegeven virtuele munten spenderen.*' In het geval van Bitcoin zijn deze regels opgenomen in de software die de participanten op hun computer of IT-infrastructuur draaien. Deze participanten in het blockchainnetwerk verifiëren dus exact deze en geen andere regels. Dit leidt in beginsel tot weinig flexibiliteit. Het zou evenwel bijzonder nuttig zijn als we een blockchainnetwerk op een flexibele manier ook allerlei regels kunnen laten afdwingen voor een diverse set van toepassingen. Blockchaingebaseerde smartcontracttechnologie laat ons toe dat die regels gedistribueerd, zonder centrale partij, worden afgedwongen. Vaak komt het neer op het volgende: '*Transfereer activa, maar pas nadat aan bepaalde voorwaarden voldaan is*'. Bijvoorbeeld: '*Betaal een vergoeding, maar enkel indien de vlucht meer dan drie uur vertraging heeft.*'[59]
Smart contracts laten dus toe om gemaakte afspraken automatisch uit te voeren, zonder daarbij een beroep te moeten doen op een gemeenschappelijke, vertrouwde tussenpartij, maar met gebruik van een bestaand, generiek blockchainnetwerk[60]. Eén enkel

58 V. Buterin, 'DAOs, DACs, DAs and More: An Incomplete Terminology Guide', *Ethereum blog*, 6 mei 2014, https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide.

59 Zie Verordening (EG) nr. 261/2004 van het Europees Parlement en de Raad van 11 februari 2004 tot vaststelling van gemeenschappelijke regels inzake compensatie en bijstand aan luchtreizigers bij instapweigering en annulering of langdurige vertraging van vluchten en tot intrekking van Verordening (EEG) nr. 295/91.

60 Zie T.F.E. Tjong Tjin Tai, 'Smart contracts en het recht', *NJB* 2017/146, p. 176-182; T.J. de Graaf, 'Van oud naar nieuw: van internet naar smart contracts en van mensen naar code', *WPNR* 2018 nrs. 7199 en 7200, p. 494-501 en 525-530; E. de Vries, 'Smart contracts: een keten van vertrouwen reikend tot in de fysieke wereld', *NTBR* 2019/12; L.A. DiMatteo, M. Cannarsa & C. Poncibò, *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, Cambridge University Press 2019; M. van der Linden, 'Het recht geketend: Smart contracts: dé oplossing voor gezeur, gedoe en onzekerheid?', *Tijdschrift voor Internetrecht* 2018/2, p. 61.

blockchainnetwerk kan dus instaan voor de uitvoering van een heel diverse set smart contracts. Niemand kan daarbij de correcte uitvoering van een smart contract eenzijdig beïnvloeden. In toenemende mate zouden hierdoor, in theorie, geschillen en dus ook de nood aan een rechterlijke tussenkomst kunnen verdwijnen.

De term 'smart contract' bestaat al langer en werd voor het eerst gebruikt door Nick Szabo midden de jaren negentig van de vorige eeuw. Hij defineert het als volgt: '*A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs*'.[61] Hij bedoelde daarmee dus technologie die ondersteuning biedt bij het uitvoeren van juridische overeenkomsten met behulp van algoritmen.[62] Een smart contract hoeft onderliggend dus geen gebruik te maken van blockchaintechnologie en hoeft zelfs niet gedistribueerd uitgevoerd te worden. Als men tegenwoordig spreekt over smart contracts, worden echter vrijwel altijd – net zoals in dit boek – blockchaingebaseerde smart contracts bedoeld.

Een blockchaingebaseerd smart contract kan virtuele munten ontvangen, vasthouden en uitgeven. Dat laatste gebeurt enkel wanneer aan bepaalde voorwaarden voldaan is. Virtuele munten maken een essentieel onderdeel uit van *publieke* smartcontractplatformen. Maar er is meer. Alle activa die op een blockchain geregistreerd en getransfereerd kunnen worden, die dus getokenizeerd zijn (*infra* 2.6. Tokens), kunnen eigenlijk door een smart contract ontvangen, geblokkeerd en getransfereerd worden. Dit kan gaan van auteursrechten en domeinnamen tot diamanten en woningen. Dit vergroot het potentieel van blockchaintechnologie dus aanzienlijk.

Samengevat is een smart contract een set van toepassingsspecifieke regels, uitgedrukt in computercode, die op een blockchain gepubliceerd worden en door het blockchainnetwerk collectief en correct uitgevoerd worden, waarbij het smart contract waarde kan ontvangen, blokkeren en transfereren. Dit laat toe om gedistribueerd, dus zonder centrale partij, afspraken tussen partijen af te dwingen. Meer bepaald dwingt een smart contract de toepassing af van de algoritmische regel '*if this, than that*'. Indien dus aan bepaalde voorwaarden wordt voldaan, vindt een bepaalde handeling of transactie plaats. 'Smart contract' is evenwel een misleidende benaming. Het is immers niet per se een 'contract' of een 'overeenkomst'. Het kan op zich het sluiten of het uitvoeren van een overeenkomst inhouden, maar dit hoeft niet. Zo kan het onder meer gaan over een verbintenis uit een eenzijdige wilsuiting, zoals bijvoorbeeld het ontslag van een werknemer, of een bestuurshandeling (bijvoorbeeld een beschikking die voortvloeit uit een

61 N. Szabo, *Smart contracts*, 1994, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

62 N. Szabo, 'Formalizing and securing relationships on public networks', *First Monday* 1997, nr. 9, https://doi.org/10.5210/fm.v2i9.548.

gebonden bevoegdheid). Het is daarnaast ook niet 'smart', maar deterministisch (*if x, than y*)[63].

## 2.2. Rechtsgevolgen van een smart contract

Een smart contract kan dus het sluiten van een overeenkomst en het uitvoeren van verbintenissen uit een overeenkomst inhouden. De overeenkomst is een rechtsfiguur uit het burgerlijk recht die leidt tot verbintenissen. Naast deze verbintenissen uit overeenkomst zijn er ook verbintenissen die ontstaan uit de wet. Artikel 6:213 lid 1 BW definieert een overeenkomst als een meerzijdige rechtshandeling, waarbij een of meer partijen jegens een of meer andere een verbintenis aangaan. Artikel 6:217 lid 1 BW bepaalt dat een overeenkomst tot stand komt door een aanbod en een aanvaarding van dat aanbod, dat wil zeggen twee eenzijdig gerichte rechtshandelingen. Een overeenkomst komt dus tot stand bij interactie die leidt tot aanbod en aanvaarding, wanneer twee of meer personen onderling jegens elkaar gedragingen verrichten waaruit blijkt of schijnt dat die personen onderling iets willen laten gelden. Algemeen wordt aangenomen dat het aangaan van een smart contract ook tot een juridische overeenkomst kan leiden.[64] Er moet wel steeds rekening gehouden worden met het feit dat specifieke wetgeving, zoals bijvoorbeeld de specifieke regels voor verkoop aan consumenten en consumentenzaken, inhoudelijke en formele geldigheidsvoorwaarden aan de overeenkomst kan toevoegen.

De relevante vraag zou natuurlijk kunnen rijzen of de betrokken partijen bij de uitvoering van een smart contract wel een rechtsgeldige op bepaalde rechtsgevolgen toegespitst aanbod en aanvaarding hebben gegeven en dus voldoende begrepen hebben wat ze juist willen laten gelden ten aanzien van elkaar. Voor niet-professionals is het immers haast onbegonnen werk om de computercode te begrijpen en werkt zo'n smart contract als het ware als een '*black box*'. Tussen personen die een overeenkomst met elkaar sluiten, wordt uitgegaan van goede trouw met betrekking tot alle elementen van de totstandkoming van de overeenkomst. Artikel 3:35 BW bepaalt dat tegen de persoon die een ander zijn verklaring of gedraging, overeenkomstig de zin die hij daaraan onder de gegeven omstandigheden redelijkerwijze mocht toekennen, heeft opgevat als een door die ander tot hem gerichte verklaring van een bepaalde strekking, geen beroep kan worden gedaan op het ontbreken van een met deze verklaring overeenstemmende wil. Tussen contracterende personen geldt dus wat deze personen in de gegeven omstandigheden redelijkerwijze uit elkaars gedragingen mochten opmaken. Bij onder-

63 Intelligentie wordt doorgaans gezien als het vermogen om kennis en vaardigheden te verwerven en toe te passen. Dit is geenszins het geval bij smart contracts.

64 UK Jurisdiction Taskforce, 'Legal statement on cryptoassets and smart contracts', november 2019, https://technation.io/about-us/lawtech-panel/; M. Schellekens, T.F.E. Tjong Tjin Tai, W. Kaufmann, F. Schemkes & R. Leenes, *Blockchain en het recht. Een verkenning van de reguleringsbehoefte*, Tilburg University, juni 2019, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/08/28/tk-bijlage-blockchain-en-het-recht-def/tk-bijlage-blockchain-en-het-recht-def.pdf, par. 3.2.8, EU Study on Blockchains - Legal, governance and interoperability aspects (SMART 2018/0038), https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038, par. 3.3.1.1.

handelingen is er sprake van een precontractuele fase waarbij de eisen van redelijkheid en billijkheid gelden, die verder zijn uitgewerkt in de jurisprudentie, en die aanleiding kunnen leiden tot het betalen van een schadevergoeding.
Drie situaties kunnen de rechtsgeldigheid van een overeenkomst in gevaar brengen en kunnen dus leiden tot nietigheid of vernietigbaarheid:[65]

– Ten eerste een *gebrekkige verklaring*, waarbij de verklaring van het aanbod niet overeenstemt met de werkelijkheid. Na afweging van bovenstaande drie beginselen kan dit leiden tot nietigheid van de overeenkomst.
– Ten tweede het *ontbreken van wil*, bijvoorbeeld in geval van geestelijke gestoordheid.
– Ten derde een *gebrekkige wil*. Een wilsgebrek, namelijk bedreiging, bedrog (art. 3:44, derde lid BW), misbruik van omstandigheden of dwaling (art. 6: 228 BW), die ertoe leiden dat de wil tot een rechtshandeling gebrekkig is gevormd, kan leiden tot de vernietiging van een overeenkomst.

Het is natuurlijk geenszins vereist noch geregeld, zelfs niet aangeraden om alle afspraken van een overeenkomst in smart contracts op de blockchain op te nemen. Een deel van de verbintenissen kan worden opgenomen in smart contracts en andere afspraken, zoals bijvoorbeeld het toepasselijke recht of de bevoegde rechter, kunnen in een gewone, schriftelijke overeenkomst worden opgenomen[66].
Naast het sluiten van een overeenkomst en het uitvoeren van verbintenissen uit een overeenkomst kan een smart contract bijvoorbeeld nog rechtsgevolgen genereren in de vorm van een opschortende of ontbindende voorwaarde van een overeenkomst[67], een eenzijdige rechtshandeling, een overheidsbesluit (in dit geval in beginsel een beschikking die voortvloeit uit een gebonden bevoegdheid), een bewijsmiddel, automatische uitvoering van (al dan niet wettelijke) processen en naleving van wettelijke verplichtingen (bijvoorbeeld het betalen van belastingen)[68].

65 M.Y. Schaub, *Wilsgebreken*, Mon. BW B3, Kluwer: Deventer 2015.
66 Zie S. Van Heukelom, J. Naves & M. Van Graafeiland, 'Whitepaper. Juridische aspecten van blockchain', *Pels Rijcken*, 7, www.pelsrijcken.nl/actueel/publicaties/whitepaper-juridische-aspecten-van-blockchain.
67 Dit zijn voorwaardelijke verbintenissen waarbij de werking van een rechtshandeling afhankelijk is gesteld van een toekomstige onzekere gebeurtenis (art. 6:21 BW). Volgens artikel 6:22 BW gaat het om een beding dat bepaalt dat de werking van een of meer bepalingen van de verbintenis in werking treden vanaf het plaatsvinden van een bepaalde onzekere gebeurtenis (opschortende voorwaarde) of vervallen (ontbindende voorwaarde).
68 Smart Contract Working Group – Dutch Blockchain Coalition, *Smart contracts as a specific application of blockchain technology*, 21-34, https://dutchblockchaincoalition.org/uploads/pdf/Smart-Contracts-ENG-report.

## 2.3. Toepassingen

### 2.3.1. *Voorbeelden*

Laat ons het voorgaande verduidelijken aan de hand van een aantal voorbeelden, namelijk smart contracts voor vastgoedtransacties, veilingen, crowdfunding, huurwaarborg, smart locks, vleestransport en verkiezingen[69]. In elk van de voorbeelden vervalt, vanuit een puur technisch standpunt, de noodzaak aan een vertrouwde autoriteit. Juridisch liggen de kaarten doorgaans wat complexer.

*- Vastgoedtransacties*
Smart contracts zouden kunnen worden ingezet in de vastgoedpraktijk (beschreven in hoofdstuk 4, Blockchain en vastgoed), met name als ook de kadastrale registratie op een blockchain zou worden geïmplementeerd. Dit zou de mogelijkheid bieden om complexe vastgoedtransacties in code te regelen, waardoor bijvoorbeeld precies kan worden geregeld wanneer en onder welke voorwaarden uitbetalingen moeten worden verricht en de eigendom van een goed wordt overgedragen.

*- Veiling*
Een veiling is een openbare verkoop waarbij volgens vastgelegde regels kan worden geboden op onroerend goed. Er zijn twee soorten: de vrijwillige veiling en de executieveiling. De laatste is een gedwongen veiling, namelijk de wettelijk voorgeschreven methode om bezittingen van een schuldenaar te gelde te maken om uit de opbrengst de vordering van de executerende schuldeiser te voldoen.
Op dit moment is het meest populaire smartcontractplatform *Ethereum*. De betrokken virtuele munt is de *ether*. Stel dat Alice in een ongereguleerde blockchainwereld een woning te koop aanbiedt door middel van een smart contract op Ethereum. Bob kan een bod plaatsen van bijvoorbeeld 4000 ether. Wanneer Bob een bod uitbrengt, stuurt hij het geboden bedrag naar het smart contract, dat dit bedrag vervolgens vasthoudt. Wanneer Bob later overboden wordt door Charlie, die een bod van 4500 ether uitbrengt, houdt het smart contract die 4500 ether vast en krijgt Bob opnieuw toegang tot de 4000 ether die hij geboden had. Pas wanneer de veiling afgelopen is, krijgt Alice toegang tot het bedrag van het hoogste bod.
De woning kan bovendien 'getokenizeerd' zijn. In zo'n geval kan de eigenaar (Alice) het token, namelijk de representatie van de waarde van de eigendom, voor de aanvang van

69 Zie M. Pomp & R. Verhaert, *Blockchain in de praktijk. Meer dan 50 use cases van de overheid in Nederland en België*, Sdu, 2018. Zie voor andere mogelijke toepassingen onder meer D. De Jonghe en V.I. Laan, 'Blockchain in de realiteit', *Computerrecht* 2017/251; J. Linnemann, 'Juridische aspecten van (toepassingen van) blockchain', *Computerrecht* 2016/218; A. Berlee, 'Pandakteregistratie van Belastingdienst naar blockchain: een verkenning', *Maandblad voor Vermogensrecht* 2018, nr. 3, 87-93; Y.S. Berepoot, 'Blockchain unchained: gevolgen van blockchain en cryptocurrency voor de faillissementspraktijk', *Tijdschrift voor Insolventierecht* 2018/34; Zie *Special issue – Blockchain and Land Registration* in *European Property Law Journal* 2017, vol. 6, nr. 3.

de veiling transfereren naar het smart contract. Het smart contract transfereert het token na het einde van de veiling dan automatisch naar de hoogste bieder.
Het bovenstaande is echter (vooralsnog) niet mogelijk in Nederland, aangezien de notaris een centrale rol speelt bij de voorbereiding, de openbare verkoop zelf van onroerende goederen en de afwikkeling ervan. In de Algemene Voorwaarden voor Executieveilingen (AVVE 2017) staan de functie en bevoegdheden van de notaris. Voor de aanvang van de veiling bepaalt en publiceert[70] de notaris de veilingvoorwaarden, waarbij meestal wordt verwezen naar de AVVE. In de mate van het mogelijke geeft de notaris informatie over het onroerend goed en de eventuele kosten. Hij is verantwoordelijk voor een goed verloop van de veiling, waarbij hij een bod bijvoorbeeld als ongeldig kan aanmerken, personen van de veiling kan uitsluiten, opnieuw tot afslag kan overgaan of de veiling afgelasten of onderbreken. De notaris heeft een beslissende stem over alle gebeurtenissen tijdens de veiling evenals de uitleg en toepassing van de veilingvoorwaarden. Ten slotte gebeurt de betaling van de koopsom en de veilingkosten via de derdengeldenrekening van de notaris, meestal binnen zes weken na de veiling. Vooralsnog speelt de notaris dus een centrale rol bij een openbare veiling, maar het voorbeeld illustreert echter wel wat technisch kan via smart contracts.

*- Crowdfunding*
Alice lanceert een project om zeeschildpadden te beschermen en wil daarbij tegen het einde van het kwartaal een bepaald bedrag ophalen. Iedereen kan (virtueel) geld in het smart contract van de crowdfunding storten. Het smart contract zorgt ervoor dat Alice toegang krijgt tot het ingezamelde bedrag, maar alleen indien op het einde van het kwartaal minstens het vooropgestelde bedrag (uitgedrukt in virtueel geld) opgehaald zou zijn. Zo niet, krijgt iedereen zijn gestorte bedrag van het smart contract terug.

*- Blokkeren huurwaarborg*
Bij het blokkeren van de huurwaarborg zijn de huurder en de verhuurder nu nog afhankelijk van een bank. Het proces voor het blokkeren en het deblokkeren is bovendien vrij omslachtig. Een smart contract zou dit kunnen vereenvoudigen en daarbij de intermediair, de bank, overbodig maken. De huurder stort de huurwaarborg in een smart contract. Het smart contract geeft het virtueel geld alleen vrij indien zowel de huurder als de verhuurder daar zijn akkoord over geeft aan het smart contract. Bij een betwisting zou een derde partij, bijvoorbeeld een rechter, nog steeds de knoop kunnen doorhakken.
We geven een aantal kanttekeningen mee bij dit voorbeeld, die enkele huidige beperkingen van de technologie illustreren.
In systemen voor virtuele munten zoals bitcoins is het mogelijk om eenvoudige scripts uit te voeren. Het blokkeren van bitcoins en het vrijgeven op het moment wanneer bijvoorbeeld twee uit een set van drie vooraf bepaalde participanten hun goedkeuring geven, was daarin al mogelijk. Bitcoin laat dus een eenvoudige vorm van smart con-

70 Zie http://veilingnotaris.nl.

tracts toe, maar biedt absoluut niet dezelfde flexibiliteit als blockchaingebaseerde smartcontracttechnologieën die later gelanceerd werden[71]. In computerjargon luidt het dat Ethereum, in tegenstelling tot Bitcoin, *Turingvolledig* (*Turing complete*) is. Dit betekent dat alles wat je op een normale computer kunt uitvoeren, in beginsel ook met een smart contract – en dus gedistribueerd – uitgevoerd kan worden.
Tokens – representaties van activa op de blockchain – zijn onbruikbaar zolang ze door een smart contract geblokkeerd worden. Ze staan dus geblokkeerd op de blockchain. Dit verschilt van de traditionele wereld. Geld op een traditionele geblokkeerde rekening is weliswaar onbruikbaar voor de huurder en de verhuurder, maar de bank heeft er wel nog steeds toegang toe en kan het bedrag ondertussen bijvoorbeeld investeren.
De koers van de meeste virtuele munten is erg volatiel en kan op een paar dagen tijd bijvoorbeeld 20% in waarde toe- of afnemen. Wanneer nu het equivalent van 1.500 EUR aan virtuele valuta geblokkeerd wordt, kan dit een paar jaar later, wanneer de huurovereenkomst beëindigd wordt, heel veel waard zijn of evengoed heel weinig. Deze onvoorspelbaarheid maakt het gebruik van dergelijke virtuele munten voor heel wat toepassingen tot op heden in de praktijk bijzonder moeilijk. Voorlopig is het nog wachten op het eerste volwassen publiek blockchainplatform voor smart contracts op basis van *stable coins* (*infra* 3.8. Koersvolatiliteit) die gekoppeld zijn aan een vaste waardedrager zoals de US dollar.

*- Smart locks*
Een intelligent slot in een wagen of een woning kan nagaan op een smart contract of de huurder van de wagen of de woning de maandelijkse huur of leasingvergoeding al betaald heeft of op zijn minst niet te veel achterstallige huur heeft. Enkel indien dit het geval is, zal het intelligente slot de huurder de mogelijkheid geven om de wagen te starten of de woning binnen te gaan. De huurder stort het bedrag in het smart contract, waarna het slot ontgrendeld kan worden. Dit idee kan uitgebreid worden, waarbij bijvoorbeeld tevens het bezit van een verzekering en een geldig rijbewijs eveneens geverifieerd worden. Via een *smart key* kan daarnaast bijvoorbeeld ook een werknemer op bepaalde tijdstippen zijn werkplek binnentreden of kan een sportvereniging gebruikmaken van een sporthal.

*- Vleestransport*
Een slager bestelt vlees bij een leverancier. Hij plaatst zijn bestelling via een smart contract, wat wil zeggen dat hij het te betalen bedrag op voorhand in het smart contract stort. In de koelwagen bevinden zich temperatuursensoren die de gemeten waarden doorgeven aan het smart contract. Indien bij levering blijkt dat de temperatuur zich steeds binnen de afgesproken waarden bevond, transfereert het smart contract het bedrag naar de leverancier. Indien dit niet het geval is, krijgt de slager zijn geld terug. Dergelijke mechanismen kunnen een aanvulling zijn op de casus van de toeleveringsketen (*infra* 5.4. Casus herkomst en toeleveringsketen).

71 *Bitcoin* werd in 2009 gelanceerd, *Ethereum* pas in 2015.

*- Verkiezingen*

Dit is een toepassing van smart contracts die geregeld wordt aangehaald. Het smart contract dwingt af dat enkel stemgerechtigden hun stem kunnen uitbrengen en dit slechts één keer. Op het einde van de stemronde geeft het smart contract het correcte resultaat. Het idee is dat verkiezingsfraude onmogelijk wordt, waarbij het blockchainnetwerk toeziet op de correcte uitvoering. Ook hier moeten een aantal belangrijke bemerkingen worden gemaakt.

We moeten kunnen garanderen dat de privacy van de burgers afdoende beschermd wordt en het constitutioneel gewaarborgde stemgeheim niet geschonden wordt.[72] Gezien het spanningsveld tussen gedistribueerd vertrouwen en confidentialiteit (*infra* 7.4. Transparantie en confidentialiteit), is dit niet evident.

In het smart contract moet geregistreerd worden wie wel en wie geen stemrecht heeft. De vraagt rijst evenwel hoe gegarandeerd kan worden dat elke stemgerechtigde correct geregistreerd is en er geen valse kiezers gecreëerd worden. Het lijkt op dat moment noodzakelijk dat elke stemgerechtigde beschikt over een digitale identiteit, die wordt gekoppeld aan de biologische identiteit door bijvoorbeeld een foto, vingerafdruk of een gezichtsscan. Hiertegen kunnen natuurlijk privacy argumenten worden geformuleerd. Daarnaast kan de overheid zich niet kwijten van de taak om erop toe te zien dat het volledige proces goed verloopt.

In het verleden, nog voor er sprake was van blockchain, werden al verschillende voorstellen voor online digitale verkiezingen uitgewerkt[73]. Daarbij was geavanceerde cryptografie nodig om aan de strenge privacy- en veiligheidsvereisten tegemoet te komen. Bij een blockchainbenadering is dit niet anders. Als we echt veilig onlineverkiezingen willen organiseren, kan blockchain daar in het beste geval een deel van uitmaken, maar zal er dus nog van alles daaromheen nodig zijn, wat het geheel erg complex maakt. Het is dan ook niet toevallig dat het stemmen in Nederland nog steeds met het potlood verloopt. Zelfs het huidige systeem om elektronisch de stemmen te tellen, zou ernstige veiligheidskwetsbaarheden bevatten[74]. In het algemeen blijft stemmen via internet dan ook controversieel. Vooral veiligheidsexperts hebben bezwaren[75]. Blockchain kan in het beste geval een deel uitmaken van het organiseren van veilige onlineverkiezingen, maar is op zich geenszins voldoende.

Dit is een fenomeen dat vaker geobserveerd kon worden te midden van de blockchainhype. Blockchain lijkt vaak, op het eerste gezicht, een eenvoudige oplossing. Zodra alles echter in detail uitgewerkt wordt, blijkt het vaak allerminst eenvoudig. Belangrijke

72 J.-H. Hoepman, *Het gebruik van blockchain technologie in het verkiezingsproces*, Radboud Universiteit, PI.lab, 12 april 2018, https://www.rijksoverheid.nl/documenten/rapporten/2018/04/12/het-gebruik-van-blockchaintechnologie-in-het-verkiezingsproces.

73 E. Magkos, P. Kotzanikolaou & C. Douligeris, 'Towards secure online elections: models, primitives and open issues', *Electronic Government, an International Journal* 2007, vol. 4, nr. 3, 249-268.

74 Tweede Kamer eist veilig elektronisch stemmen tellen bij verkiezingen 2021. *RTL Nieuws*, 31 oktober 2019, https://www.rtlnieuws.nl/nieuws/nederland/artikel/4904466/tweede-kamer-verkiezingen-stemmen-tellen-elektronisch-software.

75 D. Gross, 'Why can't Americans vote online?', *CNN*, 8 november 2011, https://edition.cnn.com/2011/11/08/tech/web/online-voting/index.html.

details worden vaak pas zichtbaar op het moment dat alles van nabij wordt bekeken en uitgewerkt.
Bovenstaande voorbeelden kunnen gezien worden als een set van afspraken die door de participanten moet worden nageleefd. Dankzij smart contracts worden deze regels afgedwongen zonder centrale partij en wordt het ontwijken van deze regels in beginsel onmogelijk.
De gegeven voorbeelden zijn vrij eenvoudig en worden frequent gebruikt om het potentieel van smart contracts uit te leggen. Er kan echter nog heel wat verder gegaan worden. In de introductie gaven we al verschillende voorbeelden van de taken van tussenpersonen die met behulp van blockchain en smart contracts gedistribueerd zouden kunnen worden. Gegeven de vele uitdagingen zal het overbodig maken van de tussenkomst van deze partijen zeker nog niet voor morgen zijn, maar zullen we eerder evolueren naar een herijking van hun rol.

### 2.3.2. *Toepassingen door de overheid en effectieve rechtsbescherming*

Ook bij de overheid zijn allerlei toepassingen denkbaar[76], waarbij het smart contract bijvoorbeeld zou kunnen leiden tot het toekennen van een subsidie. In tegenstelling tot een besluit van algemene strekking lijken smart contracts vooral een rol te kunnen spelen bij beschikkingen, namelijk besluiten met een individuele strekking. Daarnaast lijkt het gebruik van een smart contract geschikter bij een zogenaamde gebonden bevoegdheid, waarbij het bestuursorgaan in beginsel slechts één beslissing kan nemen, dan bij een discretionaire bevoegdheid met beslissingsruimte voor het bestuur. In dat laatste geval is er immers sprake van ruimte voor het bestuur met betrekking tot het al dan niet nemen van een besluit (beleidsruimte) of de inhoud ervan (beoordelingsruimte), waarbij belangen van de aanvrager, derde-belanghebbenden en het algemeen belang moeten worden afgewogen op basis van artikel 3:4, lid 1 Algemene wet bestuursrecht (Awb). Denk bijvoorbeeld aan de beoordeling of een vergunningaanvraag al dan niet in overeenstemming is met de goede ruimtelijke ordening. Een bestuursorgaan is steeds gebonden door het geldende recht en moet ook steeds de beginselen van behoorlijk bestuur (abbb) in acht nemen, zowel de beginselen gecodificeerd in de Awb als de ongeschreven abbb. Denk onder meer aan het zorgvuldigheidsbeginsel, het motiveringsbeginsel, het evenredigheidsbeginsel, het gelijkheidsbeginsel, de hoorplicht, het rechtszekerheids- en vertrouwensbeginsel. Deze beginselen kunnen een uitdaging vormen bij deterministische smart contracts in computercode die door de burger als een black box kunnen worden ervaren[77].

76 Zie M. Pomp & R. Verhaert, *Blockchain in de praktijk. Meer dan 50 use cases van de overheid in Nederland en België*, Sdu, 2018; S. Øines, J. Ubacht & M. Janssen, 'Blockchain in government: Benefits and implications of distributed ledger technology for information sharing', *Government Information Quarterly* 2017, vol. 34, nr. 3, 355-364.

77 Zie ook Smart Contract Working Group – Dutch Blockchain Coalition, *Smart contracts as a specific application of blockchain technology*, 37-39, https://dutchblockchaincoalition.org/uploads/pdf/Smart-Contracts-ENG-report.pdf. Zie ook S. Van Heukelom, 'Responsieve rechtsstaat en digitale overheid: blockchain en smart contracts', *Nederlands Tijdschrift voor Bestuursrecht* 2018/39.

De Afdeling bestuursrechtspraak van de Raad van State (ABRvS) heeft in de PAS/AERIUS-uitspraak van 17 mei 2017[78] op basis van een recht op uitleg en informatie een toetsingskader geformuleerd voor de beoordeling van geautomatiseerde besluitvormingsprocessen, *in casu* via het softwaresysteem AERIUS dat gedeeltelijk geautomatiseerde besluitvorming (*i.e* besluitvorming met algoritmische ondersteuning) mogelijk maakt bij activiteiten die stikstof uitstoten.[79] De vraag rijst immers bij dergelijke algoritmische besluitvorming of de rechtsstatelijke waarborgen, inclusief de algemene beginselen van behoorlijk bestuur, zoals legaliteit, transparantie, openbaarheid, kenbaarheid en controleerbaarheid wel voldoende zijn gewaarborgd.[80] Volgens de ABRvS kan een gebrek aan inzicht in gemaakte keuzes en gebruikte gegevens en aannames immers aanleiding geven tot een ongelijkwaardige procespositie van partijen. Zij kunnen namelijk niet nagaan op welke basis een besluit is gekomen. De Raad van State stelde dan ook:

> *'Ter voorkoming van deze ongelijkwaardige procespositie rust in dit geval op genoemde ministers en de staatssecretaris de verplichting om de gemaakte keuzes en de gebruikte gegevens en aannames volledig, tijdig en uit eigen beweging openbaar te maken op een passende wijze zodat deze keuzes, gegevens en aannames voor derden toegankelijk zijn. Deze volledige, tijdige en adequate beschikbaarstelling moet het mogelijk maken de gemaakte keuzes en de gebruikte gegevens en aannames te beoordelen of te laten beoordelen en zo nodig gemotiveerd te betwisten, zodat reële rechtsbescherming tegen besluiten die op deze keuzes, gegevens en aannames zijn gebaseerd mogelijk is, waarbij de rechter aan de hand hiervan in staat is de rechtmatigheid van deze besluiten te toetsen'.*[81]

De ABRvS heeft zich gebaseerd op de verplichting voor het bestuur om besluiten deugdelijk en op kenbare wijze te motiveren om een gelijkwaardige procespositie van partijen te garanderen. De Hoge Raad[82] en de Centrale Raad van Beroep[83] hebben zich aangesloten bij het toetsingskader van de ABRvS. Bovenstaande redenering en toetsingskader zou ons inziens kunnen worden toegepast op besluitvorming ondersteund door blockchaingebaseerde smart contracts, waar ook sprake kan zijn van een algoritmische '*black box*'. De overheid moet dus gemaakte keuzes en gebruikte gegevens en aannames *volledig, tijdig, uit eigen beweging en op een passende wijze* openbaar maken. Wat we moeten verstaan onder 'op een passende wijze' is natuurlijk de hamvraag. Ons

78 ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259.
79 Zie J. Wolswinkel, 'Het algoritme van de Afdeling: de realiteit van complex bestuursrecht', *Ars Aequi* oktober 2019.
80 T. Barkhuysen & N. Jak, 'Afdeling bestuursrechtspraak formuleert toetsingskader voor geautomatiseerde besluitvormingsprocessen (AERIUS)', *Stibbe blog*, 23 augustus 2017, www.stibbeblog.nl/all-blog-posts/environment-and-planning/afdeling-bestuursrechtspraak-formuleert-toetsingskader-voor-geautomatiseerde-besluitvormingsprocessen-aerius.
81 ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259, ov 14.4.
82 HR 17 augustus 2018, ECLI:NL:HR:2018:1316.
83 CRvB 15 mei 2019, ECLI:NL:CRVB:2019:1737.

inziens volstaat het niet om toegang te verlenen tot de computercode, maar moet deze worden vertaald in gangbare, begrijpelijke bewoordingen[84].

In de uitspraak van 18 juli 2018 heeft de ABRvS vervolgens dit toetsingskader verfijnd door een onderscheid te maken tussen maatwerk invoergegevens en standaard invoergegevens.[85] De overheid moet *maatwerk* invoergegevens, namelijk individuele gegevens die door de gebruiker zelf worden ingevoerd, uit eigen beweging op papier of anderszins waarneembaar beschikbaar stellen als op de zaak betrekking hebbende gegevens op basis van artikel 8:42 Awb. Dit laatste is immers noodzakelijk om belanghebbenden in staat te stellen te oordelen of zij zienswijzen naar voren willen brengen of in beroep willen gaan, en dus om de juistheid van de gebruikte gegevens, gemaakte berekeningen en de daarop gebaseerde aannames, keuzes en beslissingen inhoudelijk te kunnen betwisten. Deze verplichting om gegevens uit eigen beweging over te leggen geldt echter niet – althans niet zonder meer – voor de in een concreet geval gebruikte *standaard* invoergegevens die onafhankelijk zijn van het concrete geval. Het bestuur moet deze gegevens alleen verstrekken als de burger daarom vraagt.

Het is in beginsel niet evident voor de rechter als leek op technisch vlak om naderhand de rechtmatigheid van algoritmische besluitvorming te beoordelen. Goossens en De Poorter wezen er dan ook recentelijk op dat het van wezenlijk belang is voor een effectieve rechtsbescherming om te voorkomen dat enerzijds de terugtred van de wetgever ten voordele van het bestuur in de *administrative state* en anderzijds de reductie van menselijke tussenkomst en controle van het bestuur bij rigide algoritme-gedreven besluitvormingsprocessen leiden tot een vacuüm in de rechtsbescherming. Zij zijn dan ook op zoek gegaan hoe deze vicieuze cirkel kan worden doorbroken.[86]

De aanpak van deze uitdaging om tot een inhoudsvolle rechterlijke toetsing te komen van algoritmische besluitvormingsprocessen van de overheid is volgens de auteurs tweeledig.[87]

– Enerzijds moet er meer aandacht komen voor regulering aan de voorkant van het overheidsbesluitvormingsproces. Zo dient het recht op nuttige informatie en uitleg bij algoritmische besluitvorming verder te worden geconcretiseerd en geoperationaliseerd, moeten regels worden aangenomen over de omstandigheden en voorwaarden waaronder het bestuur zich mag baseren op algoritmische besluitvormingsprocessen, en kan worden gedacht aan een verplichte algoritmische impact assessment, zoals de Canadese *Algorithmic Impact Assessment* voor federale overheidsdiensten op basis van de *Directive on Automated Decision-Making*[88], en de aanstelling van een toezichthouder. Ten slotte is het aanbevolen om een onder-

84 Zie in dezelfde zin S. Van Heukelom, 'Smart contracts in het bestuursrecht. Wat eist de bestuursrechter eigenlijk van smart contracts?', *iBestuur online*, 13 februari 2018, https://ibestuur.nl/weblog/smart-contracts-in-het-bestuursrecht.

85 ABRvS 18 juli 2018, ECLI:NL:RVS:2018:2454.

86 J. de Poorter & J. Goossens, 'Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht', *NJB* 2019/44, p. 3307.

87 *Ibid*., 3312.

88 https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.

zoeksplicht voor het bestuursorgaan wettelijk te verankeren om zicht te krijgen op het collectieve effect van algoritmen.[89]

– Anderzijds vereist de verplichte heroverweging door het bestuursorgaan in de bezwaarschriftprocedure (art. 7:11, lid 1 Awb) volgens de auteurs de mogelijkheid van een menselijke heroverweging, vergelijkbaar met het recht op menselijke tussenkomst bij verwerking van persoonsgegevens zoals gewaarborgd door artikel 22 AVG (i.e. het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit waaraan voor de betrokkene rechtsgevolgen zijn verbonden of dat deze anderszins in aanmerkelijke mate treft)[90]. Ten slotte dient een effectieve rechterlijke controle van een algoritme-gedreven besluitvorming die betrekking heeft op de regulering van de voorkant dient verder te gaan dan een loutere *process-oriented* review. De rechter moet tevens de noodzakelijkheid en geschiktheid van de achterliggende algoritmische beslisregel evenals de evenredigheid van de uitwerking ervan *in concreto* kunnen toetsen, waarbij bijstand door een deskundige nodig kan zijn voor de rechter.[91]

## 2.4. Werking

Een smart contract bestaat uit computercode die de *logica* (regels) bevat. Een smart contract doet, net zoals een drankautomaat, echter niets uit zichzelf. Enkel wanneer het gevraagd wordt iets te doen, zal het reageren. Elk smart contract bevat ook een geheugen met informatie die nodig is om de logica uit te voeren. Het publiceren van het smart contract, een vraag aan een smart contract om iets te doen en, ten slotte, het vernietigen van het smart contract gebeurt telkens door middel van een blockchaintransactie die de nodige informatie bevat en op de blockchain terechtkomt. In het geval van de publicatie van een nieuw smart contract zal dit bijvoorbeeld de computercode van het smart contract zijn. Op een publiek blockchainnetwerk zoals Ethereum hangt aan dergelijke acties een prijskaartje. Het bedrag wordt uitgedrukt in de virtuele munt van het netwerk en hangt af van verschillende aspecten, waaronder de grootte van de transactie, de vereiste rekenkracht, de verzadigingsgraad van het netwerk en de gewenste snelheid van verwerking.

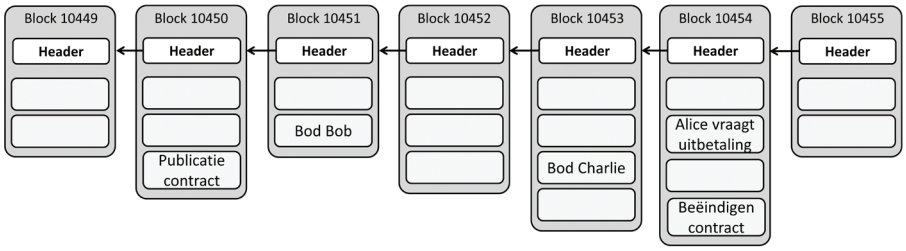
De volledige transactiegeschiedenis van het smart contract zit dus vervat in de blockchain, zoals geïllustreerd in figuur 3 voor een veilingvoorbeeld. Uit die geschiedenis kan de meest actuele toestand van het smart contract afgeleid worden, bijvoorbeeld bij een veiling wie op dit moment de hoogste bieder is en hoeveel die geboden heeft. Die toestand is het geheugen van het smart contract en wordt lokaal bijgehouden door meerdere participanten in het netwerk die lokaal een volledige, actuele kopie van de

89 J. de Poorter & J. Goossens, 'Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht', *NJB* 2019/44, p. 3312.

90 Zie N. Jak & S. Bastiaans, 'De betekenis van de AVG voor geautomatiseerde besluitvorming door de overheid. Een black box voor een black box?', *NTB* 2018/40, p. 3018-3025.

91 J. de Poorter & J. Goossens, 'Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht', *NJB* 2019/44, p. 3312.

blockchain bijhouden. Deze participanten zullen ook allen het smart contract uitvoeren (bijvoorbeeld het registreren van een bod). Als we zeggen dat een smart contract gedistribueerd op het blockchainnetwerk uitgevoerd wordt, betekent dit dus dat een heleboel participanten exact dezelfde code uitvoeren.




Figuur 3. Een blockchain met daarin de vijf transacties voor het smart contract van de veiling.

Wie kan de inhoud van dit smart contract zien? In publieke, *permissionless* blockchainnetwerken zoals Ethereum is het antwoord eenvoudig: iedereen kan inzage hebben in de code, de huidige toestand én de volledige transactiegeschiedenis van het smart contract. Afgeschermde, *permissioned* blockchainnetwerken bieden meer controle op wie wat kan zien. Ten eerste heeft slechts een geselecteerde groep participanten toegang tot de blockchain. Ten tweede kan er gebruik worden gemaakt van cryptografie om slechts bepaalde participanten in het netwerk de mogelijkheid te bieden om de code, inhoud en transactiegeschiedenis van het smart contract te kunnen zien. In zowel publieke als afgeschermde netwerken is het mogelijk te specificeren wie welke functies in het smart contract kan oproepen.

Samengevat wordt een smart contract door heel wat participanten uitgevoerd en hebben potentieel meerdere participanten inzage in de code, de huidige toestand en het verleden van het smart contract. Er is geen enkele partij in het netwerk die in haar eentje de correcte werking van het smart contract kan beïnvloeden. Een smart contract is *reactief*. Het doet niets, tenzij het expliciet gevraagd wordt iets te doen. Daartoe creëren we een transactie, een digitaal ondertekende aanvraag, die op de blockchain terechtkomt. De transacties op de blockchain vormen bijgevolg de onwijzigbare transactiegeschiedenis van het smart contract, op basis waarvan zijn meest recente toestand afgeleid kan worden. In één blockchainnetwerk kunnen heel wat verschillende smart contracts uitgevoerd worden.

## 2.5. Orakels

Een smart contract is bij wijze van spreken *doof en blind*. Het is niet 'smart', maar deterministisch en kent niets buiten zijn eigen toestand. Het heeft zelf geen toegang tot zijn transactiegeschiedenis of andere gegevens op de blockchain en kan niet zomaar de toestand van andere smart contracts te weten komen. Het heeft evenmin toegang tot gegevens uit de reële wereld of elders op internet. Toch heeft het dergelijke gegevens soms nodig. Denk bijvoorbeeld aan een verzekering voor vertragingen van vluchten.

Enkel indien een vlucht voldoende vertraging heeft of geannuleerd is, betaalt het smart contract een vergoeding uit. Daarvoor heeft het wel informatie over de vluchten uit de reële wereld nodig.
Die informatie wordt aan het smart contract aangeleverd door een zogenaamd *orakel*. Dit is een entiteit die vertrouwd moet worden, bijvoorbeeld een luchthavenautoriteit, rechter, notaris of bestuursorgaan. Het aanleveren van die informatie gebeurt via een transactie die die informatie bevat en op de onderliggende blockchain gepubliceerd wordt. Ook de geschiedenis van de aangeleverde informatie blijft voor eeuwig op de blockchain.
Een ander voorbeeld is een smart contract dat automatisch een vergoeding uitbetaalt bij geluidsoverlast. De slimme geluidssensor, het orakel *in casu*, geeft dan geregeld aan het smart contract de maximum gemeten geluidsvolumes door.

## 2.6. Tokens

Elke publieke blockchain heeft zijn eigen virtuele munt, met zijn eigen koers, die we in dit deel de *basismunt* of *native currency* zullen noemen. Ook een smart contract kan echter zijn eigen virtuele munt hebben. Op het Ethereum-smartcontractplatform heb je de ether als basismunt, maar daarbovenop heb je heel wat smart contracts die draaien met elk hun eigen munt met eigen koers. *Storj* en *FirstBlood* zijn voorbeelden van gedistribueerde applicaties die gebruikmaken van dergelijke Ethereum-smart contracts.
De organisatie of de persoon die het smart contract publiceert, definieert in het smart contract wie hoeveel van de munten bezit en eventueel ook hoe snel nieuwe munten in circulatie komen. Een deel van de munten bestaat dus vanaf de lancering van het smart contract. De nieuwe virtuele munt bestaat enkel op het niveau van het smart contract. Het is het smart contract dat steeds bijhoudt welk pseudoniem hoeveel munten bezit en het verhandelen gebeurt eveneens via het smart contract, door middel van de basismunt.
Een blockchain heeft dus zijn eigen regels en zijn eigen virtuele munt. Daarop kunnen meerdere smart contracts gepubliceerd worden, met elk een eigen set van regels en mogelijk dus een eigen virtuele munt.
Virtuele munten behoren tot de bredere categorie van tokens. Een *token* is een transfereerbare representatie van waarde op een blockchain. Er zijn verschillende manieren om tokens te classificeren, onder meer volgens hun wettelijke status, volgens de waarde die ze vertegenwoordigen, volgens hun doel, volgens hun gebruiksmogelijkheden of volgens hun technische kenmerken.[92] Toch zijn er een aantal archetypes die terugkomen:

– *Basismunt*

92 T. Euler, 'The Token Classification Framework: A multi-dimensional tool for understanding and classifying crypto tokens', *Untitled INC*, 18 januari 2018, www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/.

De basismunt wordt gebruikt als ruilmiddel en als – doorgaans volatiele – waardedrager en rekeneenheid op een specifiek blockchainnetwerk. Het is niet uitgegeven door een centrale autoriteit. Voorbeelden zijn *bitcoin* en *monero*.

– *Getokenizeerde activa*
Getokenizeerde activa representeren activa buiten de blockchainwereld zoals goud, olie of dollars. Voorbeelden zijn *PAX Gold*, *Digix Gold* en *GoldMint*, waarvan de tokens telkens gekoppeld zijn aan een vaste hoeveelheid – in de fysieke wereld moeilijk verhandelbaar – goud. Bij *Tether* is elk token gekoppeld aan één dollar.
– *Gebruikstokens*
Om gebruik te maken van een specifieke gedistribueerde dienst kun je gebruikstokens nodig hebben. Een voorbeeld is *FirstBlood,* een op smart contracts gebaseerd gaming platform waar je gebruikstokens kunt winnen door van een tegenstander te winnen en waar je gebruikstokens kunt inzetten. De gebruikstokens hebben een eigen koers, maar zijn niet bruikbaar buiten FirstBlood.
– *Aandelentokens*
Aandelentokens representeren aandelen in een bedrijf dat een ICO-verkoop (*infra* 3.14. Initial Coin Offerings) succesvol afgerond heeft. Een voorbeeld is de *tZero* ICO.

Welk pseudoniem hoeveel tokens heeft, wordt bijgehouden op het niveau van de blockchain of het smart contract. Een smart contract houdt dus koppels bij van de vorm *pseudoniem-aantal*. In het geval een token een uniek goed uit de reële wereld representeert, zoals een woning, houdt het smart contract koppels van de vorm *identificatiesleutel-pseudoniem* bij, waarbij de identificatiesleutel verwijst naar het goed, en het pseudoniem toebehoort aan de huidige eigenaar.

## 2.7. Code is law?

Een smart contract wordt ook weleens een, letterlijk vertaald, een '*intelligente overeenkomst*' genoemd. Beide termen geven evenwel ten onrechte de indruk dat het sowieso ook over een juridische overeenkomst gaat.[93] Er zijn daarnaast een aantal praktische uitdagingen, die ook tot juridische vraagstukken aanleiding kunnen geven. Hoe weten we bijvoorbeeld of de contracterende partijen werkelijk de programmeercode en dus de inhoud van de overeenkomst goed begrepen hebben? Op publieke platformen zoals Ethereum wordt daarnaast gebruikgemaakt van virtueel geld, waarvan de juridische status onzeker en fel bediscussieerd is. Bovendien zijn de meeste virtuele munten sterk onderhevig aan wisselkoersschommelingen. Op publieke smartcontractplatformen zijn de participanten bovendien doorgaans enkel gekend onder een pseudoniem en dus niet onder hun echte naam. De sleutel die hoort bij het pseudoniem kan ook gestolen of gedeeld worden. Voor *intuitu personae* overeenkomsten, waarbij de identiteit

93 Zie voor een juridische analyse van smart contracts bijvoorbeeld het special issue, *European Review of Private Law*, 2018, vol. 26, afl. 6.

van de contracterende partij bepalend is voor het sluiten van de overeenkomst, is dergelijke pseudonimiteit in ieder geval onvoldoende.
Daarnaast kan een smart contract *bugs* (programmeerfouten) bevatten[94]. Laat ons even kijken naar The DAO als concrete case. De opzet van The DAO was de creatie van meerwaarde door op een geautomatiseerde manier te investeren in allerlei projecten. Het is een soort virtuele organisatie, wat in The DAO *whitepaper* als volgt beschreven wordt[95]:

> *'[An organization] in which (1) participants maintain direct real-time control of contributed funds and (2) governance rules are formalized, automated and enforced using software.'*

Het was een set van smart contracts op Ethereum, en kan in die zin als een subsysteem binnen Ethereum gezien worden. Investeerders konden ethers naar The DAO sturen en kregen in ruil stemtokens. Meer geïnvesteerde ethers resulteerden in meer stemrecht. Projectvoorstellen konden ingediend worden met als doel een subsidie in ethers te ontvangen van The DAO. Een dergelijk voorstel had eveneens de vorm van een smart contract en kon dus ethers ontvangen en spenderen. Na het indienen van een voorstel volgde een stemronde. Bij voldoende ja-stemmen stuurt The DAO een bedrag in ether naar het project, met als doel er op termijn meer ether van terug te ontvangen. Het was een erg populair project. Op een gegeven moment hadden 18.000 investeerders er samen zowat 168 miljoen dollar in gestort, ofwel 14% van alle ethers die op dat moment in omloop waren.
Om te vermijden dat een meerderheid – uitgedrukt in stemtokens – zijn wil kon opleggen, waarbij de minderheid gedwongen zou worden om te volgen, was de mogelijkheid voorzien om The DAO te splitsen, waarbij de minderheid hun ethers kon transfereren naar een nieuw, door The DAO gecreëerd smart contract.
Helaas bevatte deze mogelijkheid om te splitsen een bug, waardoor een aanvaller – wellicht bewust – er in slaagde om 54 miljoen dollar aan ethers over te hevelen naar dit nieuw gecreëerde smart contract[96]. Zonder interventie vanuit de Ethereum community had de aanvaller deze ethers een paar weken later kunnen transfereren naar hemzelf. De aanval leek dus doelgericht, terwijl de bug in The DAO wellicht onbedoeld was. In november 2017 gebeurde iets gelijkaardigs met de *Parity bug*, waardoor 170 miljoen dollar verloren gegaan is. Net zoals The DAO werd ook dit geschreven door

94 N. Atzei, M. Bartoletti & T. Cimoli, 'A survey of attacks on ethereum smart contracts (sok)' in M. Maffei en M. Ryan (eds.), *Principles of Security and Trust, Berlijn-Heidelberg*, Springer 2017, 164-186.
95 C. Jentzsch, 'Decentralized autonomous organization to automate governance', white paper, 2016, https://lawofthelevel.lexblogplatformthree.com/wp-content/uploads/sites/187/2017/07/WhitePaper-1.pdf.
96 P. Daian, 'Analysis of the DAO exploit, Hacking Distributed', 18 juni 2016, http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/; Q. Dupont, 'Experiments in algorithmic governance: A history and ethnography of "The DAO", a failed decentralized autonomous organization', in M. Campbell-Verduyn (ed.), *Bitcoin and Beyond*, New York, Routledge, 2018, 157-177; T.F.E. Tjong Tjin Tai, 'Smart contracts en het recht', *Nederlands Juristenblad* 2017/146, p. 3-4.

personen met relatief gevestigde namen. Samengevat komen programmeerfouten dus voor, wat verregaande consequenties kan hebben.

Bovendien zijn smart contracts niet altijd makkelijk te verzoenen met de werking van het rechtssysteem[97]. In de blockchaingemeenschap hoor je bijvoorbeeld geregeld de uitspraak '*Code is law*' of '*De code is de wet*'. De computercode wordt letterlijk uitgevoerd, waardoor er geen ruimte meer is voor interpretatieverschillen tussen partijen. Het is de bedoeling dat zo geschillen worden voorkomen en er in beginsel geen nood is aan een rechter. Hoewel het overeenkomstenrecht er in beginsel van uit gaat dat wilsovereenstemming moet bestaan tussen partijen, is deze wilsovereenstemming geen fundamentele eis voor het bestaan van een overeenkomst. Geregeld zal er geen sprake zijn van een uitdrukkelijke wilsovereenstemming over alle aspecten, zodat het leidend is wat personen in de gegeven omstandigheden *redelijkerwijze* uit elkaars gedragingen mogen opmaken. Er is dus een spanningsveld tussen de automatische uitvoering van overeenkomsten op basis van de onveranderlijke code van smart contracts en de zogenaamde Haviltex-norm volgens welke de omstandigheden van het geval en verwachtingen van de partijen in beginsel leidend zijn bij de uitleg van schriftelijke overeenkomsten.[98] Het is duidelijk dat de verbintenissen die ontstaan uit een overeenkomst dus niet altijd zonder meer in een smart contract kunnen worden gegoten en automatisch op een rigide wijze kunnen worden uitgevoerd zonder dat betwisting of interpretatiegeschillen ontstaan. Partijen zouden natuurlijk wel contractueel kunnen bedingen dat een letterlijke uitvoering van de computercode de uitdrukkelijke, gemeenschappelijke bedoeling is. De rechter zal hier vervolgens in beginsel mee rekening houden in zijn beoordeling. Onder partijen geldt in beginsel contractsvrijheid en het Burgerlijk Wetboek bevat voornamelijk rechtsregels van regelend recht waar contractueel van kan worden afgeweken. Er zijn echter wel enkele regels van dwingend recht opgenomen in het BW waarvan niet bij overeenkomst kan worden afgeweken.

De rechtsgevolgen van een overeenkomst worden niet alleen bepaald door hetgeen partijen zijn overeengekomen. Artikel 6:248 BW bepaalt immers dat een overeenkomst niet alleen de door partijen overeengekomen rechtsgevolgen teweegbrengt, maar ook die welke, naar de aard van de overeenkomst, uit de wet, de gewoonte of de eisen van redelijkheid en billijkheid voortvloeien. Zo kunnen eisen van redelijkheid en billijkheid bijvoorbeeld dus leiden tot aanvulling van de overeenkomst. Een tussen partijen als gevolg van de overeenkomst geldende regel is niet van toepassing, indien dit in de gegeven omstandigheden naar maatstaven van redelijkheid en billijkheid onaanvaardbaar zou zijn.

---

97 Zie C. Millard, 'Blockchain and law: Incompatible codes?', *Computer Law & Security Review* 2018, nr. 34, 843-846; G. Governatori, F. Idelberger, Z. Milosevic, R. Riveret, G. Sartor & X. Xu, 'On legal contracts, imperative and declarative smart contracts, and blockchain systems', *Artificial Intelligence and Law* 2018, vol. 26, nr. 4, 377-409; M. Schellekens, T.F.E. Tjong Tjin Tai, W. Kaufmann, F. Schemkes & R. Leenes, *Blockchain en het recht. Een verkenning van de reguleringsbehoefte*, Tilburg Universiteit, juni 2019, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/08/28/tk-bijlage-blockchain-en-het-recht-def/tk-bijlage-blockchain-en-het-recht-def.pdf, par. 3.2.8.

98 Zie J.B. Schmaal & E.M. van Genuchten, 'Smart contracts en de Haviltex-norm', *Tijdschrift voor Internetrecht* 2017/1.

Het is ook mogelijk dat er een onbedoelde uitvoering plaatsvindt. Een onbedoelde uitvoering wordt niet per se onmiddellijk ontdekt en kan door diverse factoren veroorzaakt worden, zoals het gebrek aan correctheid van de code (*bugs*), het ontbreken van correctheid van de aangeleverde data door orakels (foute invoer), onvoorzienbare gebeurtenissen, en voorzienbare maar niet-gecodeerde gebeurtenissen. Ook bij een onbedoelde uitvoering, waarbij het smart contract iets anders doet dan bedoeld en een contracterende partij zich benadeeld voelt, moet deze naar de rechter kunnen stappen om een correcte uitvoering van de overeenkomst of een schadevergoeding te eisen. De code is dus ondergeschikt aan de wet en een beroep op de rechter moet in beginsel mogelijk zijn.

Verschillende situaties kunnen de algehele rechtsgeldigheid van een overeenkomst in gevaar brengen en kunnen dus leiden tot nietigheid of vernietigbaarheid: gebrekkige verklaring, ontbreken van wil en gebrekkige wil (*supra* 2.2. Rechtsgevolgen van een smart contract).[99] Nietigheid werkt van rechtswege en vindt dus automatisch plaats. Zij kan door contracterende partijen en derden worden ingeroepen. Een nietige rechtshandeling wordt geacht nooit te hebben bestaan en heeft dus geen rechtsgevolg. Een vernietigbare rechtshandeling daarentegen heeft wel rechtsgevolg tot zolang de vernietiging wordt uitgesproken op vraag van bij de overeenkomst betrokken partijen, bijvoorbeeld in het geval van handelingsonbekwaamheid. Op basis van artikel 3:32 lid 2 BW is een rechtshandeling van een onbekwame immers vernietigbaar. Een eenzijdige rechtshandeling van een onbekwame, die evenwel niet tot een of meer bepaalde personen gericht was, is echter nietig. Een rechtshandeling is daarnaast bijvoorbeeld ook nietig bij strijdigheid met de goede zeden of de openbare orde (art. 3:40 BW); bij schending van voorgeschreven vormvereisten voor een rechtshandeling, indien bijvoorbeeld is voorgeschreven dat een rechtshandeling schriftelijk moet gebeuren, maar deze enkel mondeling heeft plaatsgevonden; opname van een beding dat wettelijk, op straffe van nietigheid, niet in een overeenkomst mocht worden opgenomen, voornamelijk ter bescherming van de zwakkere partij bijvoorbeeld bij een huur-, arbeids- of consumentenovereenkomst).

Voor de praktijk zijn de regels inzake onredelijk bezwarende bedingen belangrijker: zulke bedingen zijn eveneens nietig of vernietigbaar.[100] De code van een smart contract kan echter wel zulke bedingen bevatten, zoals een regel die de wederpartij de vrijheid geeft om al dan niet na te komen.

Om aan de regeling betreffende nietigheid en vernietigbaarheid te voldoen moet het smart contract regels bevatten die het mogelijk maken de overeenkomst terug te draaien, wat mogelijk is door transacties aan de blockchain toe te voegen die eerdere transacties ongedaan maken. Als het smart contract zulke regels niet bevat zal er in geval van nietigheid of vernietigbaarheid strijd zijn met het recht.

99 M.Y. Schaub, *Wilsgebreken*, Mon. BW B3, Deventer, Kluwer, 2015.

100 Vanwege Europese rechtspraak moeten zulke bedingen op een specifieke manier worden behandeld die enigszins afwijkt van hoe Nederlands recht met nietigheid en vernietigbaarheid omgaat.

Om al deze redenen zijn interventiemechanismen wenselijk. Dergelijke mechanismen zouden een bevoegde instantie (bijvoorbeeld een rechter of een notaris) de mogelijkheid kunnen bieden om, indien nodig, in te grijpen in de werking van het smart contract. Indien het niet gaat om een basismunt en de tokens dus beheerd worden in een smart contract, is dit technisch nog mogelijk. Bij een onrechtmatige transfer van tokens zou een bevoegde instantie het recht gegeven kunnen worden om bepaalde transacties ongedaan te maken. Wanneer echter ten onrechte door het smart contract een hoeveelheid van de basismunt uitgegeven is, kan de transactie niet teruggedraaid worden zonder medewerking van de ontvangende partij. Dit valt immers buiten de invloed van het smart contract, maar speelt zich af op het niveau van het onderliggende blockchainnetwerk. In zo'n geval kan overwogen worden om logica in het smart contract te voorzien dat de uiteindelijke transactie in de basismunt uitgesteld wordt, maar dat de bevoegde instantie wel ogenblikkelijk geïnformeerd wordt. Zo krijgt deze de kans om alsnog in te grijpen. Alternatief kan worden voorzien dat een expliciete goedkeuring van deze instantie aan het smart contract vereist is. Dergelijke maatregelen staan natuurlijk wel op gespannen voet met de oorspronkelijke snelle, geautomatiseerde en gedistribueerde doelstelling van blockchain. Bovendien introduceert het een bijkomende kwetsbaarheid. Een hacker zou mogelijks immers de sleutel van de bevoegde instantie kunnen stelen en zo mogelijks een grote controle krijgen over het smart contract. Hoe een smart contract dergelijke interventiemechanismen kan aanbieden zonder afbreuk te doen aan het gedistribueerde karakter, de veiligheid en efficiëntie is vooralsnog onduidelijk. Sowieso zijn een set van *best practices* bij het opstellen en beheer van smart contracts onontbeerlijk.

Smart contracts en hun tokens hebben vele verschijningsvormen en afhankelijk daarvan zal bepaalde specifieke wetgeving van toepassing zijn. Zo kan een smart contract gebruikt worden voor civielrechtelijke handelingen (bijvoorbeeld een huurcontract, een testament of een koopovereenkomst), maar het kan evengoed gebruikt worden voor bestuursrechtelijke handelingen (bijvoorbeeld het verlenen en weigeren van vergunningen en subsidies) of voor het naleven van fiscale verplichtingen (bijvoorbeeld een smart contract dat automatisch de te betalen belasting afhoudt en doorstort naar de Belastingdienst). Telkens zal de toepasselijke regelgeving van toepassing zijn en moeten worden nageleefd. Een algemene set van regels zal dus op juridisch vlak vaak niet volstaan voor elk specifiek geval. Vooraf zal eerst moeten worden nagegaan wat de toepasselijk regelgeving is en welke impact die heeft op het blockchainnetwerk en de toepasselijke smart contracts. Het is dus aangeraden om deze juridische analyse uit te voeren en te zorgen voor *compliance by design* alvorens een blockchaintoepassing effectief op de wereld los te laten.

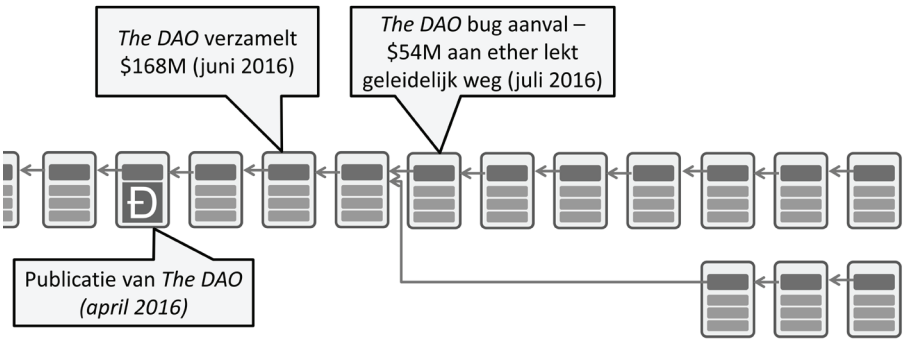
## 2.8. Aansprakelijke actoren in de blockchain

Het aansprakelijkheidsvraagstuk is ongetwijfeld een andere belangrijke juridische uitdaging.[101] Er zijn immers mogelijk heel wat verschillende entiteiten betrokken bij de ontwikkeling en de uitvoering van een smart contract, zoals de ontwikkelaar van het smart contract, de opdrachtgever voor wie het smart contract ontwikkeld werd, het orakel of de orakels die informatie aanleveren aan het smart contract, de gebruiker van het smart contract (die al dan niet opzettelijk eventueel gebruikmaakt een smart contract met een bug), de participanten in het blockchainnetwerk die een lokale kopie van het smart contract bijhouden en lokaal het smart contract uitvoeren, alsook de ontwikkelaars van het smartcontractplatform waarop het smart contract gepubliceerd werd.
Wie aansprakelijk is, zal natuurlijk geval per geval bekeken moeten worden, maar het is wel van belang om een onderscheid te maken tussen publieke en private blockchainnetwerken. Op een publiek blockchainnetwerk zijn de participanten vaak enkel gekend onder een pseudoniem, wat het moeilijker maakt om de identiteit van mogelijk aansprakelijke personen te achterhalen. Zo kunnen zelfs smart contracts onder een pseudoniem gepubliceerd worden, zonder dat we weten wie zich achter dat pseudoniem bevindt. In een privaat blockchainnetwerk kan de identiteit van elke participant achterhaald worden en kunnen duidelijke afspraken gemaakt worden wat betreft contractuele aansprakelijkheid. Sommige blockchains worden gelanceerd door een community, een groep van personen met een gedeelde interesse of doel, terwijl achter andere blockchains een bedrijf zit. In een private, *permissioned* blockchain zal het identificeren van de aansprakelijke producent in beginsel gemakkelijker zijn.
Eén smart contract kan bovendien problemen veroorzaken op het onderliggende blockchainplatform, wat op zijn beurt de uitvoering van de andere smart contracts op dat platform kan bemoeilijken. Dit leidt tot een moeilijke aansprakelijkheidsvraag. Zo was het smart contract *CryptoKitties* in december 2017 zo populair dat het onderliggende platform (Ethereum) verzadigd raakte, waardoor transactievergoedingen stegen. Het gebruik van elk smart contract op het platform, en dat waren er toch een paar honderd, werd dus duurder en trager[102].
Een tweede interessant voorbeeld waarbij een smart contract impact heeft op heel wat andere smart contracts is *The DAO*, een set van smart contracts die we in 2.7. Code is law? al vermeld hebben en verder bespreken in 2.10. Gedecentraliseerde autonome organisaties. Door een bug verdween meer dan 50 miljoen dollar uit het contract naar de aanvaller. Velen uit de Ethereum-community hadden virtueel geld in The DAO geïnvesteerd, en wilden dat natuurlijk niet zomaar verliezen. De meerderheid van de

101 Zie M. Schellekens, T.F.E. Tjong Tjin Tai, W. Kaufmann, F. Schemkes & R. Leenes, *Blockchain en het recht. Een verkenning van de reguleringsbehoefte*, Tilburg Universiteit, juni 2019, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/08/28/tk-bijlage-blockchain-en-het-recht-def/tk-bijlage-blockchain-en-het-recht-def.pdf, par. 3.2.9.

102 J.I. Wong, 'The ethereum network is getting jammed up because people are rushing to buy cartoon cats on its blockchain', *Quartz*, 4 december 2017, https://qz.com/1145833/cryptokitties-is-causing-ethereum-network-congestion.

participanten in het Ethereum netwerk ging dan ook akkoord om via een eenmalige uitzondering op de regels de gevolgen van de aanval ongedaan te maken.
Een beperkte groep participanten weigerde echter deze uitzondering. Dat resulteerde in een split (*fork*) van de blockchain in twee takken: in de zwaarste tak is de aanval ongedaan gemaakt, in de lichtere tak niet (zie figuur 4). Als de Ethereum-blockchain splitst, splitsen ook de actieve contracten mee. Stel dat er een veiling met behulp van een smart contract lopende was, dan kan elke tak een eigen hoogste bieder en een eigen hoogste bod hebben. Er stellen zich hier dus vragen omtrent de uitvoering en finaliteit van smart contracts.




Figuur 4. De Ethereum-blockchain splitst. De lichtere tak, waarin de aanval niet ongedaan gemaakt is plaatsgevonden heeft (boven), bestaat nog steeds onder de naam Ethereum Classic; de veel zwaardere is de officiële Ethereum-tak (onder).

De uitvoering van de regels in blockchaingebaseerde smart contracts zijn dus niet zo absoluut als soms beweerd wordt. Het is bovendien niet uit te sluiten dat de lichtere tak in het voorbeeld hierboven alsnog uitdooft. Het is dus correcter om te stellen dat niemand éénzijdig de regels kan overtreden in de veronderstelling dat geen enkele entiteit (of samenwerkende groep van entiteiten) meer dan 50% van de rekenkracht of de inzet controleert in het geval van *permissionless* blockchains. In dat geval kunnen de collectieve regels immers wel degelijk overtreden worden.
In dergelijke situaties, waarbij een bug in één smart contract een impact heeft op alle actieve smart contracts op het blockchainplatform – plots waren er immers twee versies van elk smart contract – stelt zich opnieuw de vraag naar aansprakelijkheid. Wie is er verantwoordelijk voor de bug in het smart contract? Wie is er verantwoordelijk voor de geleden schade die is veroorzaakt? In november 2017 werd niet ingegrepen toen 170 miljoen dollar aan ether door een bug voor eeuwig bevroren raakte op het Ethereum-platform[103]. Toch zijn *splits* niet uitzonderlijk voor publieke blockchainnetwerken. Ook Bitcoin kende meerdere splits. De reden van de *forks* is dat de regels gebaseerd zijn op consensus in de community. Wanneer er niet langer consensus is, krijgen we een split in de community en dus ook in de blockchain. In één tak is er consensus

103 A. Hern, '$300m in cryptocurrency' accidentally lost forever due to bug', *The Guardian*, 8 november 2017.

over één bepaalde set van regels, in de andere is er consensus over een andere set van regels.
Er zijn dus regels op twee niveaus: 1) de regels waarover consensus bestaat op het niveau van het platform en 2) de regels die beschreven staan in het smart contract. Ten slotte benadrukken we dat dergelijke splits niet voorkomen in private, afgeschermde blockchainnetwerken. Ook in meer centraal beheerde netwerken zoals Ripple zijn splits veel minder waarschijnlijk. Naarmate een blockchain netwerk minder gedistribueerd is, verkleint de kans op dergelijke splits. In die zin is sterke distributie van vertrouwen niet per se een voordeel.
Met betrekking tot aansprakelijkheid zou het nuttig kunnen zijn om op basis van de rol die iemand inneemt in de blockchain, bijvoorbeeld *nodes* (*i.e.* participanten van de blockchain die lokaal een blockchainkopie bewaren op hun computer en die up-to-date houden door telkens de nieuw gecreëerde blokken toe te voegen) of *miners* (*i.e.* delvers die deelnemen aan de competitie tussen een deel van de participanten om als eerste een nieuwe blok te creëren, waarbij de winnende delver nieuw gecreëerde virtuele munten en transactievergoedingen als beloning krijgt), de aansprakelijkheid duidelijk af te bakenen. Dit zou dus vrij vergelijkbaar zijn met de regeling van rechten en plichten in de AVG die worden afgebakend op basis van de rol die iemand vervult, namelijk verwerker *vs.* verwerkingsverantwoordelijke (*infra* hoofdstuk 6, Privacywetgeving)[104]. Dit kan worden overgelaten aan zelfregulering in het blockchainnetwerk, maar hier wordt misschien ook best nagedacht over een wettelijke regeling.
Bij een *permissioned*, private blockchain moeten op voorhand goede, contractuele afspraken worden gemaakt met betrekking tot aansprakelijkheid, maar bijvoorbeeld ook met betrekking tot intellectuele eigendomsrechten, verwerking van persoonsgegevens, toepasselijk recht en de bevoegde rechtbank[105]. Bij *permissionless*, publieke blockchains ligt dit moeilijker, hoewel contractuele afspraken niet onmogelijk zijn. Mits het geldende nationale recht met betrekking tot aanvaarding in acht wordt genomen, kan dan worden gedacht aan algemene voorwaarden waarnaar wordt verwezen en die deel uitmaken van de overeenkomst en aan toetredingsovereenkomsten[106].

## 2.9. Ricardiaanse contracten: smart legal contracts

Meer ingewikkelde smart contracts vereisen dat computertaal en menselijke taal gecombineerd worden. Dergelijke combinatie werd voor het eerst in 1996 beschreven door Ian Grigg, lang voor er van blockchain sprake was en kreeg de naam *Ricardiaans contract*. Grigg definieert het als volgt: '*a Ricardian contract is a digital contract that contains all necessary terms and clauses and is readable both by people and by computer*

104 E. Valgaeren & J.J. Linneman, 'Inleiding – Blockchain ontketend', *Computerrecht* 2017/250, p. 3-4.
105 M. Van Eersel & T. Van Den Bergh, 'Blockchain en smart contracts: toegang tot een reeks van slimme dingen', *Tijdschrift financieel recht in de praktijk* 2017/4, p. 47.
106 E. Valgaeren & J.J. Linneman, 'Inleiding – Blockchain ontketend', *Computerrecht* 2017/250, p. 4-5.

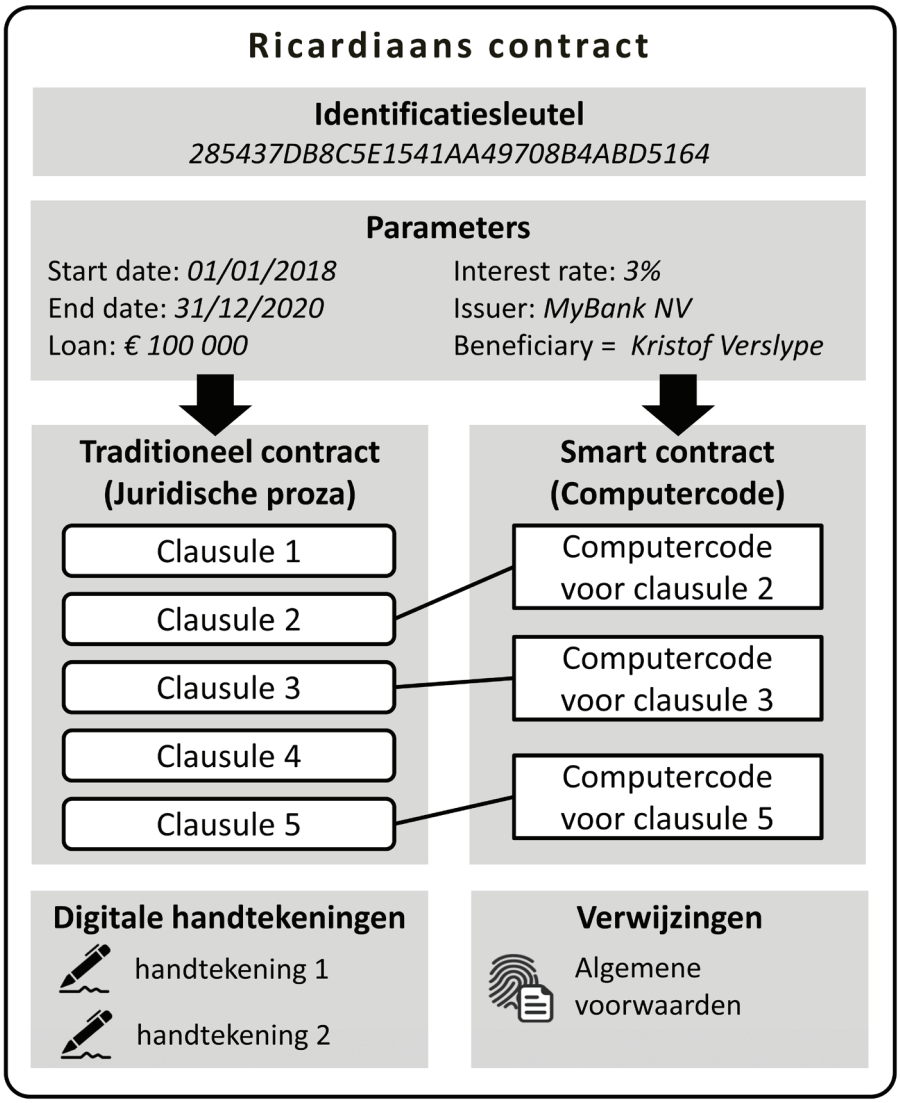
*programs, and computer programs may subsequently execute this contract if required.*'[107, 108] Blockchain en smart contracts zorgen voor een praktische manier om een dergelijk contract uit te voeren.

Een Ricardiaans contract is een overeenkomst, in de vorm van één enkel document, die zowel menselijke taal als computercode combineert, digitaal ondertekend wordt en een unieke identificatiesleutel heeft. Figuur 5 illustreert een Ricardiaans contract. Clausules uit het traditionele contract zijn gekoppeld aan de bijhorende computercode, wat het gevaar van de 'black box' (je geeft input, er vindt een proces plaats en vervolgens is het afwachten welke output eruit komt) vermindert. De code in het smart contract kan sterk variëren in complexiteit. In het meest eenvoudige geval worden enkel beweringen van de contracterende partijen onweerlegbaar en niet antedateerbaar in de blockchain geregistreerd. *Natural language processing* (NLP) als vorm van *Artificial Intelligence*, heeft in elk geval moeite met het omzetten van complexe contractuele clausules in rigide, automatisch uitvoerbare gecodeerde regels.

Naast een correcte, geautomatiseerde uitvoering biedt een op blockchaintechnologie gebaseerd Ricardiaans contract transparantie: we kunnen zien wanneer welk deel van het smart contract uitgevoerd werd, wat handig kan zijn voor audits en bij betwistingen. Dankzij de blockchain kan het contract, noch de uitvoeringsgeschiedenis gewijzigd of geantedateerd worden.

107 I. Grigg, 'The Ricardian Contract', *Proceedings of the First IEEE International Workshop on Electronic Contracting*, IEEE, 2004, 25-31, http://iang.org/papers/ricardian_contract.html.

108 U. Chohan, 'What is a Ricardian Contract?', *Cyberspace Law eJournal: Social Science Research Network*, 11 december 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3085682.




Figuur 5. Illustratie van een Ricardiaans contract.

Om een Ricardiaans contract op te stellen, vertrekken we idealiter vanuit een sjabloon – een leeg Ricardiaans contract als het ware – waaraan enkel nog parameters toegevoegd moeten worden zoals bij een lening bijvoorbeeld het te lenen bedrag, de interestvoet en de looptijd. Deze parameters worden automatisch ingevuld in zowel de juridische overeenkomst als in het smart contract. Verwijzingen naar andere documenten kunnen door middel van een hash (unieke vingerafdruk) ervan in het Ricardi-

aans contract opgenomen worden, wat garandeert dat ook deze ongewijzigd blijven. Het smart contract wordt gepubliceerd op een afgesproken blockchain platform. De contracterende partijen geven alle hun goedkeuring door middel van een digitale handtekening. Ten slotte is er de afhandeling, waarbij het smart contract uitgevoerd wordt.

Aangezien een onbedoelde uitvoering, bijvoorbeeld door een bug in het smart contract, nog steeds mogelijk is, stelt zich de vraag hoe we het risico daarop kunnen minimaliseren. Een mogelijkheid zou zijn om te werken met auditors die een smart contract controleren en verklaren dat het contract correct is. Indien er alsnog iets verkeerd zou lopen, zou de auditor aansprakelijk kunnen worden gesteld. Een dergelijke aanpak lijkt wel enkel nuttig voor frequent voorkomende overeenkomsten of overeenkomsten waar een groot financieel belang mee gemoeid is, zodat het de kosten van een audit waard is. Het lijkt niet zinvol om gewone benoemde overeenkomsten in het algemeen door de overheid beschikbaar te laten stellen in smart contract vorm. Zelfs voor een koopovereenkomst zijn er zo veel mogelijk variaties en gevallen dat het praktisch onmogelijk is om alle soorten koop op passende wijze te regelen.[109] Zoiets als wanprestatie is bijvoorbeeld onmogelijk om helemaal automatisch te regelen op dezelfde manier als dit volgens het recht verloopt, omdat het daarbij nodig is om vast te stellen wat de werkelijke oorzaak is van de niet-nakoming.[110] Er zal dan toch weer een menselijk orakel nodig zijn, wat in feite betekent dat er een vorm van arbitrage of bindend advies wordt ingebouwd in het contract.

Ricardiaanse contracten worden ook wel *smart legal contracts* genoemd. Ze worden in de praktijk nog maar zelden gebruikt en er wordt nog volop onderzoek naar gedaan. Toch zou het in de toekomst een nuttig instrument kunnen worden. Bedrijven die werken rond smart legal contracts zijn onder meer *Monax*[111] en *Clause*[112].

Mogelijk komen er ook hulpmiddelen die de complexiteit van smart contracts (en Ricardiaanse contracten) afschermen voor de schrijver ervan. Zo zou het een toegevoegde waarde zijn om smart contracts te kunnen maken puur in een grafische omgeving, waarbij de auteur niet in contact komt met code. Het nadeel is dat de auteur dan maar moet vertrouwen op de ontwikkelaar van zo'n omgeving of hulpmiddel. Verder wordt er gewerkt aan methodes om de correctheid van smart contracts te bewijzen (*formal verification*).

*The European Union Blockchain Observatory and Forum* maakt in een thematisch rapport een onderscheid tussen '*smart legal contracts*' en '*smart contracts with legal implications*'.[113] De eerste zijn smart contracts die effectief een juridisch bindende overeen-

109 Nog los van het probleem dat er dan één smart contract systeem wordt bevoordeeld, en dat het nodig is ieder contract te controleren zodra het systeem wordt gewijzigd (d.w.z. nieuwe regels worden ingevoerd).

110 T.F.E. Tjong Tjin Tai, 'Force Majeure and Excuses in Smart Contracts', *European Review of Private Law*, 2018/6, p. 787-804.

111 https://monax.io.

112 https://clause.io/.

113 T. Lyons, L. Courcelas & K. Timsit, *Legal and regulatory framework of blockchains and smart contracts*, The European Union Blockchain Observatory and Forum, 27 september 2019, 23, https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf.

komst (beogen te) representeren en de laatste zijn artefacten of constructies die andere juridische implicaties met zich meebrengen, bijvoorbeeld het oprichten van een DAO of het representeren van waarde in digitale vorm. Dit onderscheid draagt ons inziens niet echt bij tot een beter begrip van smart contracts en hun juridische waarde.

## 2.10. Gedecentraliseerde autonome organisaties

Met de komst van smart contracts op een blockchain begonnen sommigen al te dromen van *gedecentraliseerde autonome organisaties* (DAO's) op publieke blockchains. Een DAO is in wezen een bedrijf dat enkel bestaat uit één of een aantal smart contracts op een blockchain[114]. Het bedrijf heeft geen management, personeel of hoofdzetel. Door het ontbreken van dit laatste heeft een DAO dus geen fysieke locatie en is deze dus niet verbonden aan een staat. De DAO neemt beslissingen aan de hand van de regels in het smart contract. Het zou onder meer zelf kunnen beslissen om nieuwe smart contracts aan te maken of om met andere, al bestaande smart contracts te interageren (handel te drijven). Bovendien kan iedereen de code, status en transactiegeschiedenis van het smart contract inspecteren, wat leidt tot transparantie.
Een eerste voorbeeld hebben we al hiervoor vermeld, namelijk *The DAO*, een set van in mei 2016 gepubliceerde smart contracts. Investeerders konden er stemrecht kopen en met dat stemrecht meebeslissen of een bepaald project al dan niet ondersteund zou worden door The DAO. Om toch nog een connectie te hebben met de juridische structuren in de reële wereld werd in Zwitserland een bedrijf *DAO.Link* geregistreerd. The DAO bevatte evenwel een bug, wat onmiddellijk ook haar einde inluidde.
Het is niet abnormaal dat een eerste experiment geen volledig succes is. In de toekomst zouden dus zeker nog andere, succesvolle en meer complexe DAO's kunnen ontstaan, waarbij sommige geen connectie met de reële wereld zullen hebben. Het is immers perfect mogelijk dat een anoniem gepubliceerde DAO een succes wordt. DAO's zijn op zich een revolutionair, disruptief concept. Voorheen was het technisch onmogelijk dat een organisatie zou bestaan zonder personeel of fysieke vestigingsplaats, maar toch autonoom beslissingen zou kunnen nemen en transacties zou kunnen doen. Zowel vanuit technisch als juridisch oogpunt zal er ongetwijfeld nog heel wat inkt vloeien over dergelijke constructies.

## 2.11. Conclusie

Dit hoofdstuk ging dieper in op smart contracts, die het technisch mogelijk maken om afspraken tussen partijen die elkaar niet volledig (hoeven te) vertrouwen, automatisch en zonder vertrouwde tussenpartij uit te voeren aan de hand van vooraf bepaalde computercode.

114 Zie uitgebreid Allen & Overy, *Decentralized Autonomous Organizations*, juli 2016, www.allenovery.com/SiteCollectionDocuments/Article%20Decentralized%20Autonomous%20Organizations.pdf.

Hoewel smart contracts theoretisch heel wat mogelijkheden bieden, zijn er nog aanzienlijke uitdagingen, zowel technisch, juridisch als economisch. Bovendien is de naam '*smart contract*' verwarrend, aangezien het gaat om deterministische regels en er niet per se sprake is van een juridische overeenkomst (smart legal contract) waarbij verbintenissen tot stand komen.

Een smart contract is trouwens niet in staat om menselijke interpretatie door bijvoorbeeld een rechter te vervangen en het bestaande wettelijke kader blijft steeds van toepassing. Enkel het gebruik van code zal sowieso vaak te rigide zijn. Smart contracts moeten dan ook veelal als een deel of aanvulling van eerder dan een vervanging van juridische overeenkomsten worden gezien. In dit kader is het toekomstige concept van Ricardiaanse contracten, dat het beste uit beide werelden combineert, interessant. Op een iets langere termijn zouden mogelijk ook succesvolle gedecentraliseerde autonome organisaties (DAO's) kunnen ontstaan.

Indien de opkomst van blockchain, smart contracts en Ricardiaanse contracten zich doorzet, wordt het onvermijdelijk voor juristen om hun kennis op dit vlak bij te schaven. Zowel voor de betrokken partijen als voor de rechter die mogelijke geschillen moet beslechten, is het belangrijk te vermijden dat een smart contract een black box vormt waar leken op technisch vlak amper iets van verstaan. Ricardiaanse contracten lijken op dit vlak interessante mogelijkheden te bieden, maar correcte omzetting van juridische taal naar rigide, automatisch uitvoerbare code zal niet steeds evident zijn.

# 3. Toepassing: virtuele munten

*'Not so long ago, some experts argued that personal computers would never be adopted, and that tablets would only be used as expensive coffee trays. So I think it may not be wise to dismiss virtual currencies. […] We must welcome their potential but also recognize their risks.'*[115]

Christine Lagarde, (voormalige) *managing director* IMF

## 3.1. Introductie

Wanneer een persoon met fysiek geld betaalt, is het evident dat die euro maar één keer uitgegeven kan worden, om de simpele reden dat de persoon in kwestie die euro niet langer bezit. In de digitale wereld ligt dit echter wat moeilijker. Hoe kan vermeden worden dat iemand een kopie van de digitale munt achterhoudt en nog een tweede (en zelfs derde) keer uitgeeft? Dit noemt men het *double spend*-probleem. In het huidige elektronische betalingsverkeer is dit de taak van een bank als centrale tussenpersoon. Bitcoin slaagde er echter als eerste in om dit probleem op te lossen *zonder centrale tussenpartij*.

Bitcoin gebruikt daarvoor onderliggend een blockchain en was de eerste blockchain-toepassing. Het werd in 2008 beschreven door een persoon (of groep personen) die we enkel kennen onder het pseudoniem *Satoshi Nakamoto*. In 2009 werd het daadwerkelijk gelanceerd. De timing was niet toevallig na de bankencrisis van 2008, op een moment dat het vertrouwen in de bankensector zich op een dieptepunt bevond en mensen bang waren hun spaargeld op de bank te verliezen. Dankzij Bitcoin werden financiële transacties over internet mogelijk zonder de banken, die zogenaamd te traag zouden zijn, hoge commissies opstrijken en niet te vertrouwen zijn. Dankzij Bitcoin kon je vanaf dan voor een lage kost nationale en internationale transacties uitvoeren die snel verwerkt werden.

Voor velen sprak vooral de astronomische waardestijging van bitcoins tot de verbeelding. Op 22 mei 2010 kocht een softwareontwikkelaar naar verluidt twee pizza's voor 10.000 bitcoins. Eind december steeg de waarde van 1 bitcoin tot 20.000 dollar. Op het moment van schrijven is de waarde van de bitcoin sterk afgenomen, maar bedraagt

115 C. Lagarde, 'Addressing the Dark Side of the Crypto World', *IMF Blog*, 13 maart 2018, https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world.

deze nog steeds meerdere duizenden dollars. Indien de pizzeria ze nog steeds bezit, zijn die 10.000 bitcoins ondertussen tientallen miljoenen waard.
Er zijn ondertussen dan ook heel wat systemen en andere digitale munten die op Bitcoin geïnspireerd zijn. Denk aan Bitcoin Cash, Litecoin, Ethereum en Ripple en het bij Facebook in de steigers staande Libra. Hoewel de term *cryptocurrencies* of cryptogeld het meest gangbaar is, heeft onder andere de ECB het liever over virtuele valuta of virtuele munten. De ECB definieert virtuele valuta of virtuele munten als volgt:

> *'A digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money.'*[116]

In de hedendaagse complexe economie is er nood aan een flexibel monetair beleid, terwijl tegelijkertijd de inflatie onder controle moet worden gehouden. Een belangrijk instrument van de centrale banken is de hoeveelheid geld die in omloop is. Dit instrument ontbreekt bij virtuele munten. Ook schaalbaarheid is essentieel. Een stijgend aantal financiële transacties in het systeem mag niet resulteren in oplopende kosten. Virtuele munten hebben op dit moment nog een beperkte capaciteit, gaande van een paar tot een paar duizend transacties per seconde. Transactiekosten kunnen sterk fluctueren bij virtueel geld naargelang vraag en aanbod. Indien vele transacties ongeveer gelijktijdig verwerkt moeten worden, zal dit een opwaartse druk op de transactiekosten zetten, aangezien de capaciteit van het netwerk op korte termijn vrij stabiel en beperkt blijft. Op het moment van schrijven spreken we voor Bitcoin over een maximumcapaciteit van een tiental transacties per seconde, Ethereum (optimistisch geschat) een 25-tal en Ripple 1.500 per seconde, terwijl VISA 65.000 transacties per seconde aankan. Op het hoogtepunt van de Bitcoin-hype eind 2017 was er enorm veel vraag om bitcoin-transacties te verwerken. Het netwerk raakte verzadigd en het daggemiddelde voor de transactiekosten steeg tot 55 dollar. Op het moment van schrijven, fluctueert dit rond de halve dollar, onafhankelijk van de geografische afstand tussen zender en ontvanger en onafhankelijk van de grootte van het bedrag.
Volgens de winnaar van de Nobelprijs voor de Economie in 2008 Paul Krugman, zijn de hoge transactiekosten van gedistribueerde virtuele munten zoals bitcoins samen met de volatiliteit van de koers een stap terug in de tijd:

> *'Cryptocurrency enthusiasts are effectively celebrating the use of cutting-edge technology to set the monetary system back 300 years. Why would you want to do that? What problem does it solve? I have yet to see a clear answer to that question. [...] Gold does have real-world uses, both for jewelry and for things like filling teeth, that provide a weak but real tether to the real economy. Cryptocurrencies, by contrast, have no*

116 Europese Centrale Bank (ECB), *Virtual currency schemes – A further analysis*, Frankfurt am Main, ECB, 2015, www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

> *backstop, no tether to reality. Their value depends entirely on self-fulfilling expectations — which means that total collapse is a real possibility.'*[117]

Ook de *Bank for International Settlements* (BIS) is bijzonder kritisch voor virtuele munten zoals bitcoins, veel kritischer dan bijvoorbeeld het IMF:

> *'Cryptocurrencies promise to replace trusted institutions with distributed ledger technology. Yet, looking beyond the hype, it is hard to identify a specific economic problem which they currently solve. [..] Transactions are slow and costly, prone to congestion, and cannot scale with demand. The decentralised consensus behind the technology is also fragile and consumes vast amounts of energy [...] A combination of a bubble, a Ponzi scheme and an environmental disaster.'*[118]

Dit hoofdstuk bespreekt virtuele munten en neemt daarbij de meest populaire munt bitcoin als uitgangspunt. We bespreken de werkingsprincipes, de risico's, de regulering en het gebruik. Veel van wat we hier bespreken over bitcoins is eveneens van toepassing op heel wat andere virtuele munten, waarvan er ondertussen meer dan 2.000 bestaan[119]. Honderden andere virtuele munten waren echter slechts een kort leven beschoren en hielden op te bestaan[120]. Op het moment van schrijven schommelt de totale waarde van al deze virtuele munten rond de 200 miljard dollar. Maar liefst 68% van die waarde wordt vertegenwoordigd door bitcoin en 90% door slechts tien virtuele munten. Van de 2000 virtuele munten zijn er trouwens op het moment van schrijven minder dan 400 met een dagvolume boven 1000 dollar. Er zijn dus maar een paar dominante, veel kleinere en vooral veel verwaarloosbare virtuele munten.

## 3.2. **Principe**

Het Bitcoin-netwerk is gedistribueerd, wat betekent dat elke participant met een beperkt aantal andere participanten verbonden is en samen de betalingsdienst aanbieden zonder de tussenkomst van een centrale partij. Bitcoin maakt onderliggend gebruik van een blockchain. Het netwerk voegt dus collectief nieuwe blokken van transacties toe aan de blockchain, gemiddeld elke 10 minuten. Heel wat participanten (*nodes*) bewaren lokaal een blockchainkopie en houden die up-to-date door er telkens het nieuw gecreëerde blok aan toe te voegen. Bitcoin is gebaseerd op het Proof of Work (PoW) consensusmechanisme, wat het principe van *minen* of delven impliceert (*supra* 1.5. Consensusmechanisme).

---

117 P. Krugman, 'Transaction Costs and Tethers: Why I'm a Crypto Skeptic', *The New York Times*, 31 juli 2018, www.nytimes.com/2018/07/31/opinion/transaction-costs-and-tethers-why-im-a-crypto-skeptic.html.

118 P. Amery, 'Cryptocurrencies may end up in the money graveyard, warns the BIS', *New Money Review*, 17 juni 2018, www.newmoneyreview.com/index.php/2018/06/17/cryptocurrencies-may-end-up-in-the-money-graveyard-warns-the-bis.

119 CoinMarketCap, 'All Cryptocurrencies', https://coinmarketcap.com/all/views/all.

120 www.coinopsy.com en https://deadcoins.com.

De Bitcoin-blockchain is op het moment van schrijven zowat 260 GB groot. Gelukkig hoef je om bitcoins te versturen of te ontvangen de blockchain niet te downloaden. Er wordt namelijk een onderscheid gemaakt onder de participanten in de *blockchain* tussen *full nodes* en *light nodes*. Een *full node* houdt een volledige kopie van de Bitcoin-blockchain bij. Wanneer het een nieuw blok ontvangt, verifieert de blockchain of het blok in orde is. Het verifieert meer bepaald of aan alle regels voldaan is. Enkel in dat laatste geval wordt het blok immers aan de lokale kopie van de blockchain toegevoegd en verder doorgestuurd op het netwerk. *Full nodes* dragen zo mee bij tot het gedistribueerd veilig houden van de blockchain. *Light nodes* gebruiken *Simplified Payment Verification* – en worden daarom ook SPV-*nodes* genoemd. Zij houden per blok slechts zeer beperkte informatie bij, wat op het moment van schrijven gecumuleerd neerkomt op ongeveer 50 MB. Dit volstaat om te verifiëren of specifieke transacties aanvaard zijn. Typisch zal een smartphone enkel een *light node* bevatten.

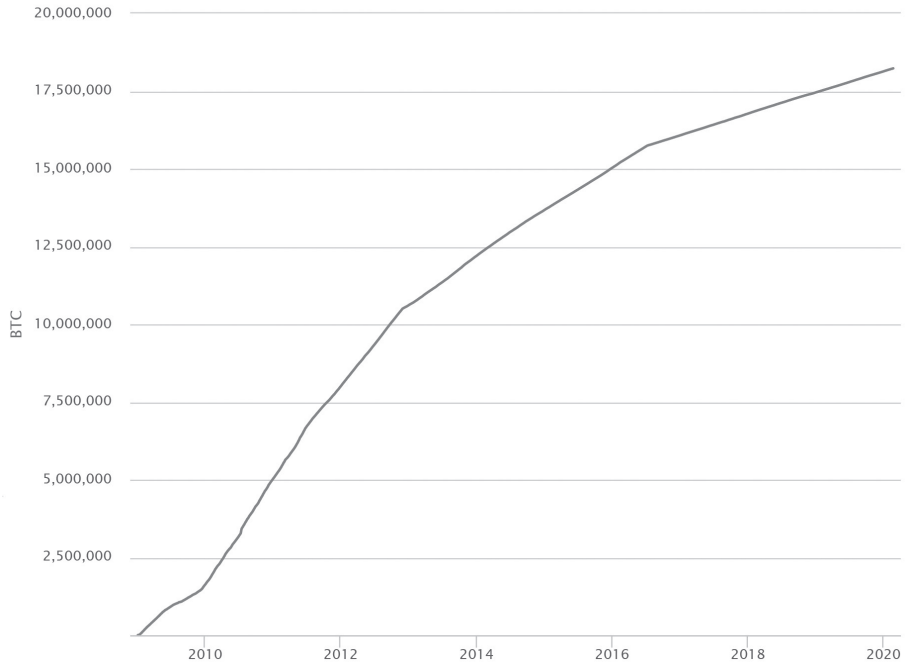
## 3.3. Transparantie

Het Bitcoin-netwerk, net zoals vele andere netwerken voor virtuele munten, is publiek en *permissionless*, wat betekent dat er geen toetredingsvoorwaarden zijn en iedereen alle transacties kan zien. Iedereen wereldwijd kan dus transacties verrichten of trachten bitcoins te delven. Iedereen kan de blockchain downloaden van andere participanten in het netwerk en zo de volledige Bitcoin-geschiedenis te weten komen. Die transparantie zorgt voor veiligheid, aangezien iedereen op deze manier kan nagaan of alles correct verlopen is, onder meer of niemand eenzelfde bitcoin twee keer uitgegeven heeft (geen *double spend*). We weten ook exact hoeveel bitcoins elk pseudoniem (*adres* in Bitcoin-terminologie) bezit, de financiële geschiedenis van zulk pseudoniem en welke weg een bitcoin afgelegd heeft. Bitcoin en de meeste andere virtuele munten zijn dus niet anoniem, maar pseudoniem, wat gepaard gaat met identificatierisico's.

## 3.4. Het nieuwe goud?

Net zoals het ontginnen van goud, vergt ook de creatie van een nieuw, geldig blok zeer veel energie. Het vereist immers het oplossen van een moeilijke, cryptografische puzzel. Denk hierbij aan een soort unieke *rubic cube* per blok. De delvers in het netwerk gaan in competitie met elkaar om deze puzzel als eerste op te lossen. Het blok van de winnaar wordt door het netwerk aanvaard en participanten voegen het nieuwe blok toe aan hun lokale kopie van de blockchain. De winnaar krijgt als beloning momenteel 12,5 nieuw gecreëerde bitcoins, wat ergens in mei 2020 zal halveren tot 6,25. Daarnaast ontvang de winnaar ook transactievergoedingen voor elke transactie in het blok. Die gecombineerde beloning is groot als je weet dat de actuele waarde van 1 bitcoin duizenden dollars bedraagt. Net zoals een goudzoeker hoopt een Bitcoin-delver bij elk nieuw blok geluk te hebben en iets te vinden. De kans dat je wint, is ongeveer proportioneel met je aandeel in de totale computerkracht in het Bitcoin-netwerk. In de praktijk is de

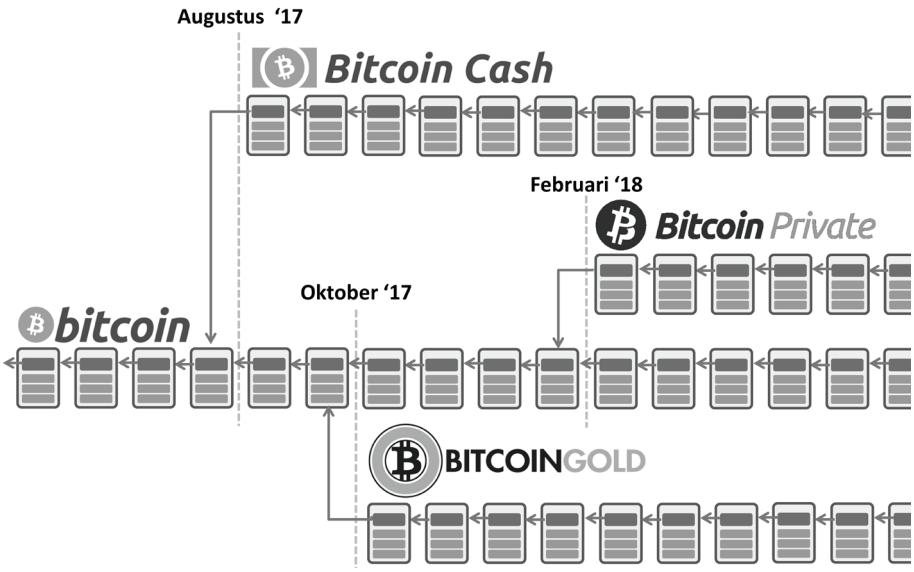
verdeling weliswaar niet helemaal evenredig, aangezien grote delvers een voordeel genieten.
Net zoals bij goud, is ook het aantal bitcoins beperkt en wordt het steeds moeilijker om de overblijvende te delven. Elke vier jaar halveert het aantal nieuw gecreëerde bitcoins per blok (zie figuur 6). Ergens rond 2140 zou de laatste gedolven worden, waardoor de enige overblijvende inkomstenbron voor de delvers de transactievergoedingen zullen zijn. Hoe snel en hoeveel bitcoins in circulatie komen, is een collectieve regel die zich bevindt in de Bitcoin-software, die door heel veel participanten gebruikt wordt.




Figuur 6. Evolutie van het theoretisch aantal bitcoins in circulatie.

Het functioneren van het Bitcoin-netwerk is gebaseerd op consensus over bepaalde regels. Hoe groot mag een blok zijn? Hoe snel komen nieuwe bitcoins in circulatie? Hoe wordt de moeilijkheidsgraad van de cryptografische puzzel bepaald? Soms gebeurt het echter dat een deel van de Bitcoin-gemeenschap het niet eens is met de regels en dan zijn eigen weg gaat. Op zulk moment zien we dat de onderliggende blockchain zich splitst, zoals geïllustreerd in figuur 7, waarbij elk van de takken onderhouden wordt door zijn eigen *community*. Dit noemt men in blockchaintermen een *fork* of een *split*. In augustus 2017 ontstond zo *Bitcoin Cash*, in oktober van datzelfde jaar *Bitcoin Gold*, in februari 2018 *Bitcoin Private* en in november van dat jaar *Bitcoin SV*. Elk van de virtuele munten heeft zijn eigen koers en elk van de netwerken bezit een andere hoeveelheid geaccumuleerde delfcapaciteit, wat tevens resulteert in een verschillend

niveau van veiligheid. De originele Bitcoin heeft nog steeds onbetwist zowel de hoogste koers als de grootste hoeveelheid geaccumuleerde delfcapaciteit.




Figuur 7. De Bitcoin-blockchain en drie aftakkingen.

Een vreemd neveneffect van een split is dat de al bestaande virtuele munten meesplitsen. Stel dat u midden 2017 één bitcoin had en deze het daaropvolgende jaar niet uitgegeven heeft, dan beschikte u eind 2018 naast uw één bitcoin ook over een muntje Bitcoin Cash, een muntje Bitcoin Gold, een muntje Bitcoin Private en een muntje Bitcoin SV. Elk van deze munten kan weliswaar slechts één keer uitgegeven worden, en dit enkel op de corresponderende blockchaintak. De reden is dat de transactiegeschiedenis, de blockchain dus, tot op het moment van de aftakking gedeeld wordt. Het is in die geschiedenis dat geregistreerd staat hoeveel muntjes iedereen bezit. Het kan ook steeds zijn dat één of meerdere takken na een tijdje afsterven, omdat er geen delvers meer zijn die er hun energie willen insteken, omdat het niet langer voldoende winstgevend is. De bijhorende muntjes verdwijnen in dat geval bijgevolg ook.
Elk van de vijf virtuele munten uit de vorige paragraaf is even zeldzaam en ze hebben alle gelijkaardige eigenschappen. Het is dus alsof je op de tabel van Mendelejev (i.e. het periodiek systeem) plots vier nieuwe elementen krijgt die sterk gelijken op goud en even zeldzaam zijn als goud. Bovendien zijn er ondertussen meer dan honderden virtuele munten die allemaal zeldzaam zijn en die allemaal wel in meer of mindere mate op bitcoins lijken. Anderzijds verschillen ze ook allemaal van elkaar. Ze zijn immers bijvoorbeeld niet allemaal even veilig en gedistribueerd, sommige beschermen de privacy beter, andere laten smart contracts toe of maken gebruik van andere concepten.

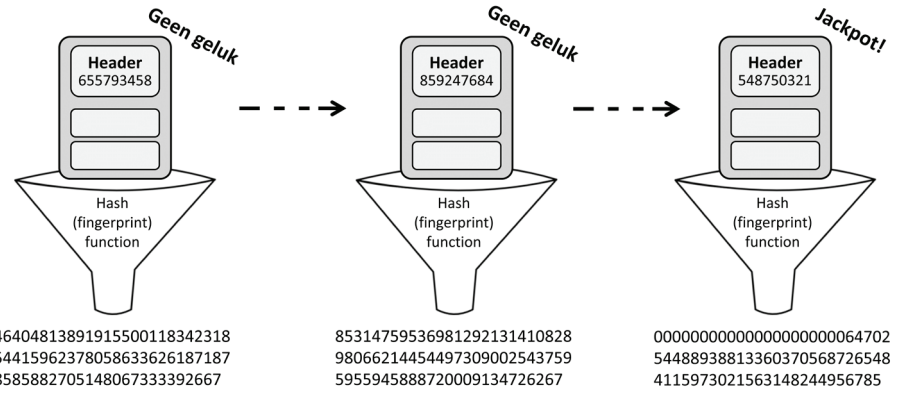
Zeldzaam hoeft trouwens niet te betekenen dat er op een gegeven moment geen munten meer in omloop gebracht worden, zoals bij Bitcoin. Er zijn andere virtuele munten waarbij enkel de jaarlijkse hoeveelheid nieuwe munten die in omloop gebracht worden, beperkt is. Dogecoin, bijvoorbeeld, brengt jaarlijks 5 miljard nieuwe muntjes in omloop. Dit beoogt het tegengaan van oppotten en speculatie en het stimuleren van gebruik van de virtuele munt voor waardeuitwisselingen in plaats van speculatie.
Hoe snel virtuele munten van een bepaald type in omloop gebracht worden, ten slotte, is slechts een collectieve regel. Er is dus geen cryptografische, maar enkel een speltheoretische[121] garantie dat die regel nooit verandert. Of anders gezegd: in het – momenteel misschien onwaarschijnlijke, maar niet-ondenkbare – geval dat de *community* (de gemeenschap) rond de virtuele munt vindt dat het beter is de regel te veranderen, zal dat ook gebeuren.
'Zeldzaam' moet dus worden genuanceerd. In theorie is er geen enkele beperking op het aanbod van virtueel geld.

## 3.5. Ecologische impact

Populaire systemen voor virtuele munten zoals Ethereum en Bitcoin maken gebruik van het energie-intensieve PoW-consensusmechanisme en hebben daardoor een aanzienlijke ecologische voetafdruk. Bitcoin spant op dat vlak de kroon. Volgens schattingen van Digiconomist[122] verbruikt het Bitcoin-netwerk op het moment van schrijven ongeveer evenveel elektriciteit als Oostenrijk of ongeveer 64% van het Nederlandse elektriciteitsverbruik. Volgens die schatting zijn er maar 39 landen met een hoger elektriciteitsverbruik dan Bitcoin (104 landen voor Ethereum) en is de Bitcoin $CO_2$-uitstoot vergelijkbaar met die van Denemarken. Daarvoor krijgen we thans slechts een tiental transacties per seconde in de plaats.
Door de lage prijs van de elektriciteit in China vindt de meeste delfactiviteit daar plaats. Volgens recente schattingen zou het gaan om 65% van de totale delfcapaciteit[123]. De voornaamste bron voor elektriciteit in China is echter nog steeds vervuilende steenkool. Bitcoins hebben dus een stevige ecologische voetafdruk. Ook waterkracht op basis van stuwdammen speelt er weliswaar een belangrijke rol in de elektriciteitsvoorziening, maar dergelijke stuwdammen hebben een enorme impact op de omgeving[124].
Hoe werkt het PoW-consensusmechanisme? PoW impliceert, zoals aangegeven, het principe van *minen* of delven (*supra* 1.5. Consensusmechanisme). De hash (*supra* 1.3. Wat is blockchain?) van een blok is een getal van 32 bytes lang. In dit blok is er een

121 Speltheorie is een techniek om situaties met strategische interacties tussen verschillende beslissingsnemers te analyseren en de uitkomst te voorspellen. We analyseren welke keuzes een speler heeft en hoe de uitkomst van die keuze beïnvloed wordt door de keuze van andere spelers. Zie K. Leyton-Brown & Y. Shoham, *Essentials of Game Theory – A Concise Multidisciplinary Introduction*, Morgan and Claypool Publishers, 2009.
122 Digiconomist, *Bitcoin Energy Consumption Index*, https://digiconomist.net/bitcoin-energy-consumption.
123 'The Bitcoin mining network. Trends, average creation costs, electricity consumption & sources', *CoinShares Research*, December 2019, https://coinsharesgroup.com/research/bitcoin-mining-network-december-2019.
124 'The Downside of Dams: Is the Environmental Price of Hydroelectric Power Too High?' *Scientific American*, 18 september 2012, https://www.scientificamerican.com/article/how-do-dams-hurt-rivers/.

getal dat de *miner* moet vinden dat de hash van het resulterende blok voldoende klein maakt[125], zoals geïllustreerd in figuur 8. Het vinden van dit getal gebeurt door een willekeurige waarde te kiezen, de hash van het blok (met daarin dus dat getal), te berekenen en na te gaan of die hash voldoende klein is. Is dit niet zo, dan doen we die oefening nog eens over voor een ander willekeurig getal. Alle *miners* in het netwerk doen onafhankelijk van elkaar hetzelfde, maar met andere, willekeurig gekozen getallen. Geaccumuleerd, door alle *miners* samen, wordt deze oefening op het moment van schrijven ruim 100.000.000.000.000.000.000 keer per seconde (ofwel honderd miljard miljard keer per seconde) gedaan. Er is een collectieve regel in de Bitcoin-software die bepaalt hoe klein de hash van een blok moet zijn. Dit wordt berekend aan de hand van de snelheid waaraan de blokken in het recente verleden gecreëerd werden. Indien dit sneller is dan één blok per tien minuten, zal de moeilijkheidsgraad stijgen. Indien dit trager is, daalt ze. Iedereen in het netwerk die een volledige kopie heeft van de blockchain kan dus autonoom die moeilijkheidsgraad berekenen. Dit mechanisme houdt de snelheid waaraan nieuwe blokken gecreëerd worden min of meer constant. Hoewel het oplossen van de cryptografische puzzel enorm moeilijk is, is het verifiëren gemakkelijk en efficiënt. Een participant hoeft slechts eenmaal de hash van een blok te berekenen en na te gaan of het resultaat kleiner is dan een bepaald getal.




Figuur 8. Een miner of delver probeert als eerste een getal in het blok te vinden zodat de hash ervan voldoende klein is. Dit komt ruwweg neer op een een hashwaarde die begint met voldoende nullen.

## 3.6. Nieuw concept, oude technologie

Bitcoin wordt gezien als iets totaal nieuws, als iets revolutionair. Het is inderdaad een nieuw concept, maar wel één dat voortbouwt op principes die soms al tientallen jaren

125 Dit is enigszins inaccuraat, maar volstaat voor een begrip van het basisprincipe. Voor een gedetailleerde technische uiteenzetting van Bitcoin verwijzen we naar A. Narayanan, J. Bonneau, E. Felten, A. Miller & S. Goldfeder, *Bitcoin and Cryptocurrency Technologies – A Comprehensive Introduction*, Princeton: Princeton University Press 2016.

oud zijn, wat als een eeuwigheid kan beschouwd worden in de computerwereld. Vele van de gebruikte concepten komen uit de moderne cryptografie, die zijn deed intrede begin jaren 1970.

Al in 1983 slaagde David Chaum erin met cryptografie een protocol te ontwikkelen voor anoniem elektronisch geld. Sterker nog, de anonimiteitseigenschappen waren sterker dan die van Bitcoin en bovendien was het mogelijk gestolen elektronisch geld ongeldig te maken. Wel was er nog steeds een centrale partij in het hele verhaal vereist, die in beperkte mate vertrouwd moest worden[126]. Het concept had dan ook niet de revolutionaire ambitie banken overbodig te maken. Het is dat idee dat een cruciale rol speelde in het succes van Bitcoin.

Acht jaar later, in 1991, verscheen in de *Journal of Cryptology* een artikel getiteld *How to time-stamp a digital document* dat wel zeer hard doet denken aan een blockchain die toelaat om zaken onweerlegbaar en met datering te registreren in een gegevensstructuur die door meerdere partijen collectief veilig gehouden wordt[127]. Het liet weliswaar niet toe om waarde uit te wisselen, maar het onweerlegbaar registreren wordt wel gezien als een van de grote voordelen van blockchaintechnologie.

De onderdelen van het in 2008 gelanceerde Bitcoin bestonden dus eigenlijk al ten minste vijftien jaar. Hoewel het bijgevolg op zich mogelijk zou zijn geweest om het Bitcoin-idee al vijftien jaar eerder te publiceren, was het op dat moment nog niet praktisch haalbaar om het idee daadwerkelijk in de praktijk te gebruiken. Dit valt niet alleen te verklaren door de beperktere opslag-, verwerkings- en communicatiecapaciteit, maar ook door de lagere efficiëntie van de toen gebruikte cryptografische instrumenten, zoals bijvoorbeeld voor digitale handtekeningen.

In 2008 werd dus het Bitcoin-concept gepubliceerd. In vergelijking met de academische cryptografische publicaties op dat moment was de Bitcoin-publicatie opmerkelijk eenvoudig. Het lijkt waarschijnlijk dat de toegankelijkheid van het concept heeft bijgedragen aan de popularisering ervan, althans onder mensen met een informatica-achtergrond. De manier waarop de uitvinder het *double spend*-probleem aangepakt heeft, is echter wel nieuw. Daarbij wordt niet enkel gebruikgemaakt van cryptografie, maar ook van speltheorie. Dit was een breuk met de heersende benaderingen in de wereld van de cryptografie, waar alles bewijsbaar veilig moet zijn, gegeven een zo beperkt mogelijk aantal cryptografische veronderstellingen. Dit impliceert dat het concept veilig is zolang de onderliggende wiskundige aannames waarop het gebouwd is, solide zijn.

We illustreren dit laatste aan de hand van een eenvoudig voorbeeld. *RSA* is een algoritme voor onder meer digitale handtekeningen dat nog steeds populair is. Het is gebaseerd op de aanname dat er geen efficiënte manier bestaat om uit een getal dat het product is van twee grote priemgetallen opnieuw die priemgetallen te vinden. Dit is

126 D. Chaum, *Blind signatures for untraceable payments*. Advances in Cryptology Proceedings. 82 (3): 199-203. 1983. http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF.

127 S. Haber, W. & S. Stornetta, 'How to Time-Stamp a Digital Document', *Journal of Cryptology*, Vol. 3, No. 2, 1991, 99-111, https://www.anf.es/pdf/Haber_Stornetta.pdf.

nooit bewezen en dus een aanname. De dag dat iemand een manier vindt om dit wel efficiënt te berekenen, is RSA niet langer veilig en kunnen onder andere valse digitale handtekeningen gecreëerd worden. De dag dat er een voldoende krachtige kwantumcomputer is, wordt de RSA aanname eveneens ongeldig, maar volgens de meeste experts ligt dit nog een aantal decennia van ons verwijderd.
Samengevat is Bitcoin, vanuit cryptografisch oogpunt, niets om lyrisch over te worden. Het zijn eerder de disruptieve socio-economische aspecten en het ideologische verhaal die Bitcoin tot een succes gemaakt hebben.

## 3.7. Gebruik en misbruik

Virtuele valuta worden helaas niet zelden voor illegale activiteiten gebruikt[128]. Al sinds midden de jaren 1990 is het mogelijk om over internet anoniem te communiceren[129]. Met de komst van virtuele munten werd het vervolgens ook mogelijk om te betalen zonder je identiteit prijs te geven. Daarmee ontstond een tandem voor illegale handel op het *Dark Web*, een afgescheiden deel van internet dat gebruikt wordt voor criminele activiteiten. Een tweede illegale praktijk met virtuele valuta is *ransomware*. Dit is een kwaadaardige code die bestanden op een geïnfecteerde computer cryptografisch versleutelt. Enkel na het betalen van losgeld (*ransom*) in bitcoins, krijgt het slachtoffer opnieuw toegang tot zijn bestanden. Voorbeelden zijn *WannaCry*[130], *NotPetya* en *SamSam*. De Universiteit Maastricht is maar een van de vele slachtoffers en zou de afpersers effectief virtueel geld betaald hebben[131]. Virtuele munten worden daarnaast ook gebruikt voor terrorismefinanciering[132] en het witwassen van geld[133, 134]. Tientallen verdachten verschenen in Nederland al voor de rechter, vooral voor witwassen. Dat leidde onder andere tot veroordelingen tot zes jaar voor Nederlanders die tegen hoge commissies voor klanten bitcoins – vaak verdiend op het Dark Web – 'anoniem' omruilden naar cash geld[135]. Ook oplichting komt geregeld voor. Nederlandse burgers zijn

128 Voor de inzet van het strafrecht bij misbruik van Bitcoin, zie R.J. De Jong, 'Bitcoinminers, bitcoincashers, bitcoinmixers en het strafrecht', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2017/1, p. 11-16.
129 P. Syverson, R. Dingledine & N. Mathewson, 'Tor: The second-generation onion router', *Proceedings of the 13th USENIX Security Symposium*, Usenix Association, 2004, www.usenix.org/legacy/event/sec04/tech/full_papers/dingledine/dingledine.pdf.
130 S. Mohurle & M. Patil, 'A brief study of wannacry threat: Ransomware attack 2017', *International Journal of Advanced Research in Computer Science* 2017, 8(5).
131 W. Bos, 'Cyberhack: Universiteit Maastricht betaalt losgeld', *Observant*, 2 januari 2020. https://www.observantonline.nl/Home/Artikelen/articleType/ArticleView/articleId/17789/Cyberhack-Universiteit-Maastricht-betaalt-losgeld.
132 T. Keatinge, D. Carlisle & F. Keen, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, European Union, 2018, www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604970.
133 Zie 'UK: Police seize bitcoin worth £300,000 in money laundering investigation', *KYC360*, 9 januari 2018, https://kyc360.com/news/uk-police-seize-bitcoin-worth-300000-money-laundering-investigation.
134 M.D. De Andrade, 'Legal Treatment of Crypto-Coins: The Dynamics of Bitcoins and the Crime of Money Laundering', *Brazilian Journal of Public Policy* 2017, vol. 7, 44.
135 T. Besteman, 'Bitcoin gelijkgesteld met contant geld', *De Telegraaf*, 4 april 2018, https://www.telegraaf.nl/financieel/1869975/bitcoin-gelijkgesteld-met-contant-geld.

door malafide organisaties in de eerste negen maanden van 2019 alleen al al voor 1,7 miljoen euro's opgelicht bij onlineshoppen, gokken of beleggen in virtuele munten[136]. Nobelprijswinnaar voor de Economie Joseph Stiglitz is omwille van het crimineel potentieel van virtuele munten zoals bitcoins dan ook bijzonder sceptisch[137]: '*So it seems to me it ought to be outlawed. It doesn't serve any socially useful function.*' Het is dan ook niet verwonderlijk dat autoriteiten, onder meer in het Verenigd Koninkrijk[138], middelen investeren om onder meer de Bitcoin blockchain – dus de Bitcoin-geschiedenis – te analyseren met als doel criminaliteit met virtueel geld, zoals belastingontduiking, op te sporen.

Virtuele munten kunnen ook als vluchtvaluta fungeren. Een voorbeeld daarvan vinden we in Venezuela. De Venezolaanse munt, de bolivar, is samen met de Venezolaanse economie, ingestort. Voor Venezolanen leek het dan ook interessant om hun bolivars om te zetten in virtuele munten die – zeker eind 2017 – snel in waarde stegen[139]. Virtuele munten werden toen dus in zekere mate gezien als vluchtactiva. Of dit in de toekomst zo zal blijven, zal uiteraard afhangen van het vertrouwen in en het koersverloop van virtuele munten. Dit gebruik als vluchtactiva versterkt echter wel de bezorgdheid van Europese centrale banken dat virtuele valuta op lange termijn de doeltreffendheid van het monetair beleid (inflatie, langetermijnrente, geldhoeveelheid, kapitaalcontroles enzovoort) kunnen verminderen. Zodra burgers hun geld omgezet hebben in virtuele valuta, heeft de centrale bank daar immers geen vat meer op. In zekere zin wordt de mogelijkheid om waarde aan toezicht van de eigen staat te onttrekken gedemocratiseerd. Bovendien kunnen virtuele valuta door hun sterke volatiliteit bijdragen aan monetaire instabiliteit. Volgens de Europese centrale banken is op dit moment de impact ervan op het monetair beleid en de prijsstabiliteit vooralsnog verwaarloosbaar, gelet op hun momenteel kleine monetaire voetafdruk, al volgt de ECB de evoluties op de voet[140]. Venezuela heeft al een eigen virtuele munt uitgegeven[141], hoewel de totale waarde ervan op het moment van schrijven minder dan 2 miljoen dollar bedraagt en er dus bezwaarlijk van een succes gesproken kan worden. Ook in Rusland wordt met dit idee gespeeld. Bij door een overheid uitgegeven virtueel geld, garandeert de overheid dat elke virtuele munt gedekt wordt door iets van waarde. Dat kan een vat olie zijn in het geval van Venezuela of, in het geval van Rusland, een vaste hoeveelheid roebels[142] of

136 'Opgelicht?!', *NPO*, 1 oktober 2019, https://www.npostart.nl/opgelicht/01-10-2019/AT_2119891.

137 K. Costelloe, 'Bitcoin 'Ought to Be Outlawed,' Nobel Prize Winner Stiglitz Says', *Bloomberg*, 29 november 2017, www.bloomberg.com/news/articles/2017-11-29/bitcoin-ought-to-be-outlawed-nobel-prize-winner-stiglitz-says-jal10hxd.

138 D. Philips, *HMRC explains why it wants to track your Bitcoin*, Decrypt, 22 januari 2020, https://decrypt.co/17184/hmrc-explains-why-it-wants-to-track-your-bitcoin.

139 P. Laya, 'Bolivar to Bitcoin Market Hits Record $1 Million Per Day', *Bloomberg*, 18 april 2018, www.bloomberg.com/news/articles/2018-04-18/bolivar-to-bitcoin-market-hits-record-1-million-per-day.

140 C. Scheiert, *Virtual currencies – Challenges following their introduction*, maart 2016, www.europarl.europa.eu/RegData/etudes/BRIE/2016/579110/EPRS_BRI(2016)579110_EN.pdf.

141 L. Tassev, 'Venezuela to Use the Petro to Buy Auto Parts from Russia', *Bitcoin*, 4 april 2018, https://news.bitcoin.com/venezuela-to-use-the-petro-to-buy-auto-parts-from-russia.

142 H. Partz, https://cointelegraph.com/news/is-cryptoruble-back-launch-set-for-mid-2019-says-russian-blockchain-association, Coint Telegraph, 18 januari 2018, https://cointelegraph.com/news/lambos-bling-and-mansions-what-purchases-do-crypto-millionaire-make.

goud[143]. Men kan zich echter vragen stellen bij de drijfveren van deze staten. Venezuela zou zo een alternatief hebben voor zijn ineenstortende bolivar, waardoor het makkelijker aan zijn internationale betalingsverplichtingen kan voldoen. Rusland zou dan weer met zijn virtuele valuta makkelijker westerse sancties kunnen omzeilen. Toch bekijken ondertussen ook andere, grotere spelers op het wereldtoneel, zoals China[144] en de ECB[145], de mogelijkheid om eigen virtueel geld uit te geven.

Virtuele munten kunnen voor burgers en ondernemingen echter ook gewoon een goedkoper en sneller alternatief vormen voor internationale transacties. Aangezien virtuele munten evenwel geen onderscheid maken tussen lokale en internationale betalingen en niet steeds een lagere transactiekost aanrekenen voor lagere bedragen, kunnen de transactiekosten echter hoog zijn voor kleine, lokale uitgaven. Op het moment van schrijven fluctueert de gemiddelde kostprijs voor een bitcoin-transactie rond een halve dollar, onafhankelijk van het te transfereren bedrag, maar deze gemiddelde kostprijs piekte eind 2017 bijvoorbeeld op 55 dollar. De transactiekosten hangen onder meer af van de verzadiging van het netwerk en is daardoor onmogelijk te voorspellen. Ook het omwisselen bij een handelsplatform van reëel geld naar virtueel geld en omgekeerd kost bovendien tijd en geld. Andere virtuele munten dan bitcoins rekenen trouwens doorgaans beduidend lagere transactiekosten.

Virtuele muntschema's zoals die van Bitcoins bieden bovendien de mogelijkheid om in een transactie ook wat zelfgekozen data te steken, wat toelaat om het netwerk voor andere zaken te gebruiken dan de transfer van virtueel geld. Een niet wettelijk geregeld voorbeeld vinden we in Georgië, dat als archieffunctie een eigen blockchain heeft voor de registratie van vastgoedakten (*infra* hoofdstuk 4, Blockchain en vastgoed). Deze afgeschermde blockchain wordt aan een vaste frequentie verankerd in de Bitcoin-blockchain om aldus een hogere bescherming te realiseren. Daartoe wordt aan een bepaalde frequentie de unieke *fingerprint* van de eigen blockchain in een bitcoin-transactie gestoken, waardoor wijzigingen in de eigen blockchain detecteerbaar worden.

Alles bij elkaar genomen lijkt het erop dat het voornaamste legaal gebruik van de meeste virtuele munten op dit moment speculatie is. De voorzitter van de Russische centrale bank, Sergei Shvetsov, formuleerde het in oktober 2017 al als volgt[146]: '*[Virtuele currencies] gradually transformed into high-yielding assets from being means of payment*'. De tijd van de waanzinnige koersstijgingen lijkt wel wat achter ons te liggen.

143 D. Palmer, *Russian Central Bank to Consider Gold-Backed Cryptocurrency*, CoinDesk, 23 mei 2019, https://www.coindesk.com/russian-central-bank-to-consider-gold-backed-cryptocurrency.

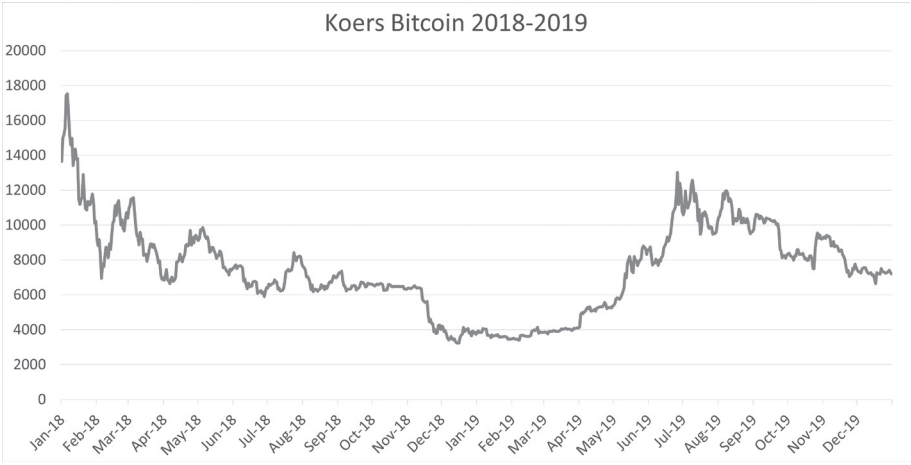
144 N. Xu Elegant, *Why China's Digital Currency Is a 'Wake-Up Call' for the U.S*, Fortune, 1 november 2019, https://fortune.com/2019/11/01/china-digital-currency-libra-wakeup-call-us/.

145 F. Guarascio, 'UPDATE 1-ECB could speed up plans for public digital currency if cash use drops', *Reuters*, 4 december 2019, https://www.reuters.com/article/ecb-cryptocurrency/update-1-ecb-could-speed-up-plans-for-public-digital-currency-if-cash-use-drops-idUSL8N28E583.

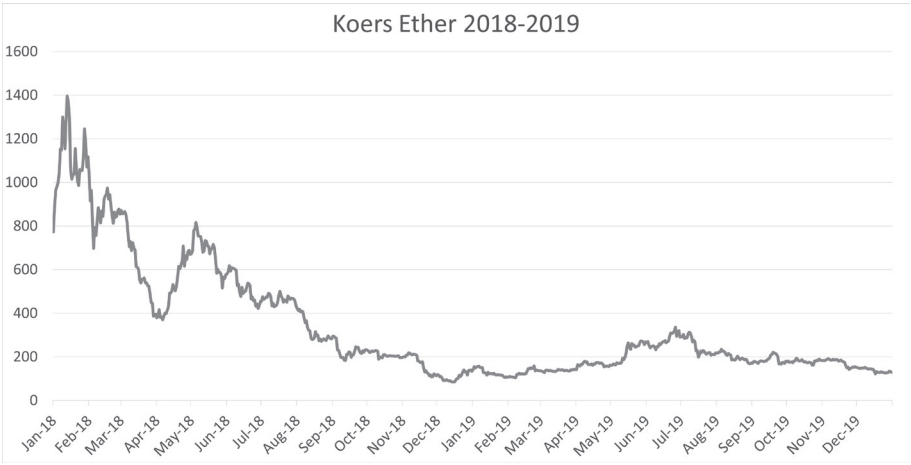
146 D. Pinchuk & E. Fabrichnaya, 'Russia turns cold on crypto-currencies', *Reuters*, 10 oktober 2018, www.reuters.com/article/us-russia-cenbank-bitcoin/russia-turns-cold-on-crypto-currencies-idUSKBN1CF0RF.

## 3.8. Koersvolatiliteit

Zoals al vermeld, is de koers van virtuele valuta bijzonder volatiel. Ze kunnen op een paar dagen 20% verliezen of winnen. Figuur 9 en figuur 10 tonen het koersverloop van de twee grootste virtuele munten: bitcoin en ether. Deze volatiliteit maakt het onmogelijk om virtuele valuta als stabiele waardedrager te zien of als rekeneenheid te gebruiken.




Figuur 9. Koers bitcoin van 01/01/2018 tot 31/12/2019.




Figuur 10. Koers ether van 01/01/2018 tot 31/12/2019.

### 3.8.1. *Flashcrash*

De koersvolatiliteit van virtuele munten neemt soms extreme proporties aan. Het komt voor dat op een handelsplatform de waarde van een virtuele munt plots implodeert, om daarna weer te herstellen. Dit is vaak het gevolg van een plotse koersdaling, bijvoorbeeld door één grote verkoop, die versterkt wordt doordat als reactie daarop klanten geautomatiseerd de virtuele munt dumpen, wat de waarde enkel verder doet instorten.

Op 22 juni 2017 kelderde de ether in enkele minuten van 300 tot 0,10 dollar op het GDAX-handelsplatform[147]. De crash werd veroorzaakt door een miljoenenverkoop, waardoor de waarde van de ether op het handelsplatform daalde van 317,81 tot 224,48 dollar. De daaropvolgende (automatische) verkopen deden de waarde verder imploderen, om daarna weer te herstellen tot de normale koers, vergelijkbaar met die op andere handelsplatformen. GDAX beloofde de gedupeerden te vergoeden[148].

Eind november 2017 vond er een andere *flashcrash* plaats op Bitfinex, één van de grootste handelsplatformen voor virtuele munten. Drie virtuele munten verloren in enkele minuten maar liefst 90% van hun waarde. Bitfinex is niet van plan de gedupeerden te vergoeden[149].

Ook het omgekeerde is mogelijk. De waarde van bitcoin op WEX, een relatief klein handelsplatform, steeg tijdelijk boven de gemiddelde marktprijs. Op 11 juli 2018 werd de bitcoin op een gegeven moment aan 9.000 dollar verhandeld, terwijl de prijs elders niet hoger dan 6.500 dollar lag. Ook de uren daarna bleef de koers op een veel hoger niveau dan het marktgemiddelde[150].

Elk handelsplatform heeft zijn eigen koers voor eenzelfde virtuele munt. Meestal liggen die erg dicht bij elkaar, maar soms zijn er dus grote verschillen. Of de gedupeerden hun geld terugkrijgen, hangt tot op heden af van de goodwill van het handelsplatform.

### 3.8.2. *Stable coins*

Een aantal virtuele munten is gekoppeld aan een stabiele waardedrager, zoals bijvoorbeeld de dollar. In dat geval spreekt men over *stable coins* of *stable currencies*. Het meest gekende voorbeeld is *Tether*, waarbij elke virtuele munt gedekt wordt door één dollar. Dit is echter moeilijk na te gaan. De ongerustheid daaromtrent maakte een audit nood-

147 A. Kharpal, 'Ethereum briefly crashed from $319 to 10 cents in seconds on one exchange after 'multimillion dollar' trade', *CNBC*, 22 juni 2017, www.cnbc.com/2017/06/22/ethereum-price-crash-10-cents-gdax-exchange-after-multimillion-dollar-trade.html.

148 W. Zhao, 'GDAX Exchange to Reimburse Traders After Ether Flash Crash', *Coin Desk*, 26 juni 2017, www.coindesk.com/gdax-exchange-reimburse-ether-flash-crash.

149 O. William-Grut, 'Anger and confusion as crypto traders lose thousands in "flash crash' on $54 billion exchange", *Business Insider UK*, 2 december 2017, http://uk.businessinsider.com/flash-crash-on-bitfinex-leaves-crypto-traders-angry-2017-12.

150 F. Memoria, 'Bitcoin Hits $9,000 on Crypto Exchange WEX Ahead Of 'Planned System Maintenance', *CryptoGlobe*, 12 juli 2018, www.cryptoglobe.com/latest/2018/07/bitcoin-hits-9000-on-crypto-exchange-wex-ahead-of-planned-system-maintenance.

zakelijk[151]. Erg gedistribueerd klinkt dit alles niet, maar de prijsvolatiliteit is in elk geval grotendeels verdwenen. De koers fluctueert doorgaans tussen de 0,99 en 1,01 dollar.
*Dai* is een *stable coin* met een andere aanpak, onafhankelijk van autoriteiten. In de plaats daarvan wordt gebruikgemaakt van speltheorie om de koers dicht in de buurt van 1 dollar te houden. Dai wordt niet gedolven. Iedereen kan Dai aanmaken, door ether als onderpand te geven. Dai is dus een soort lening in ether, met een fluctuerende interestvoet. Hoe hoger de koers van de Dai tegenover de dollar, hoe interessanter het wordt om Dai aan te maken. Dit toegenomen aanbod zet een neerwaartse druk op de koers van de Dai. Het omgekeerde gebeurt wanneer de Dai minder dan een dollar waard is. De waarde van de dollar en Dai liggen meestal minder dan 5% uiteen.
*Stable coins* kunnen ook gedeeltelijk of volledig gekoppeld zijn aan andere waardedragers, zoals bijvoorbeeld goud, wat het geval is bij onder meer *Digix Gold* en *PAX Gold*. Net zoals bij Tether zijn we hier opnieuw afhankelijk van een centrale partij die dit alles regelt en over voldoende onderpand moet beschikken.
Ook de door Facebook geplande Libra zou een *stable coin* worden, gekoppeld aan een korf van bestaande munten waaronder de Amerikaanse dollar, de Euro en de Japanse yen[152]. De Chinese Yuan is een opvallende afwezige.

## 3.9. Zijn virtuele valuta (elektronisch) geld?

De ECB maakt een onderscheid tussen verschillende vormen van virtueel geld in twee dimensies. De eerste dimensie geeft aan hoe ze verbonden zijn met de reële wereld en bestaat uit drie categorieën: 1) *gesloten virtuele muntschema's* hebben nauwelijks een link met de reële economie, 2) bij *unidirectionele virtuele muntenschema's* kunnen eenheden aangekocht worden met echt geld, maar niet opnieuw ingewisseld worden en 3) bij *bidirectionele muntschema's* kunnen eenheden van de virtuele munt ingewisseld worden in echt geld en *vice versa*. In de tweede dimensie maakt de ECB een onderscheid in hoe de virtuele muntschema's beheerd worden. Het beheer kan gecentraliseerd zijn, zoals de *Linden Dollar in Second Life*, of kan gedecentraliseerd zijn zoals in Bitcoin[153]. Als we in dit boek spreken over virtuele munten of virtuele valuta, hebben we het steeds over de meest voorkomende vorm, namelijk de gedecentraliseerde bidirectionele, die meestal op blockchain, of op het ruimere concept van *Distributed Ledger Technology* (DLT), gebaseerd zijn.
De ECB definieert virtuele valuta als: '*A digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money*'[154]. Uit deze definitie blijkt dat de ECB virtuele valu-

151 A. Irrera, 'Cryptocurrency firm Tether releases law firm report attesting to U.S. dollar reserves', *Reuters*, 20 juni 2018, www.reuters.com/article/us-cryptocurrencies-tether/cryptocurrency-firm-tether-releases-law-firm-report-attesting-to-u-s-dollar-reserves-idUSKBN1JG1SB.
152 T. Bartz, 'Facebook verzichtet bei Libra auf chinesische Währung', *Spiegel Online*, 20 september 2019, https://www.spiegel.de/wirtschaft/facebook-will-kryptowaehrung-libra-nicht-an-yuan-koppeln-a-1287853.html.
153 De ECB maakt geen onderscheid tussen gedistribueerd en gedecentraliseerd.
154 ECB, *Virtual currency schemes – A further analysis*, Frankfurt am Main, ECB, 2015, www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

ta dus niet als een volwaardige vorm van geld ziet. Virtuele valuta kunnen inderdaad economisch moeilijk als geld beschouwd worden. Virtuele valuta hebben tot op heden immers een bijzonder lage aanvaardingsgraad. Economisch gezien moet geld drie functies vervullen: het moet gebruikt worden als ruilmiddel, het moet de waarde relatief stabiel bewaren en het moet als rekeneenheid gebruikt worden. Virtuele munten vervullen deze drie criteria niet. Een belangrijke reden is de hoge graad van volatiliteit, wat conflicteert met de twee laatste functies.

Artikel 2, punt 2 Richtlijn Elektronisch geld[155] bepaalt strikt aan welke drie criteria elektronisch geld moet voldoen:

1. *elektronisch, met inbegrip van magnetisch, opgeslagen monetaire waarde vertegenwoordigd door een vordering op de uitgever;*
2. *welke is uitgegeven in ruil voor ontvangen geld om betalingstransacties als gedefinieerd in artikel 4, punt 5, van Richtlijn 2007/64/EG te verrichten;*
3. *welke wordt aanvaard door een andere natuurlijke of rechtspersoon dan de uitgever van elektronisch geld.*

In het geval van Bitcoin bijvoorbeeld is het ten sterkste de vraag of een *miner* als een 'uitgever' beschouwd zou kunnen worden en in elk geval vertegenwoordigt een bitcoin geen vordering op deze *miner*[156]. Men kan trouwens niet beweren dat virtueel geld uitgegeven wordt in ruil voor geld. Uitgifte impliceert creatie door een autoriteit. Er is *in casu* geen autoriteit en er is evenmin sprake van creatie van nieuw virtueel geld. In ruil voor geld krijgt de koper immers al bestaande virtuele munten. Ofwel werden deze al gedolven, zoals in Bitcoin, ofwel zijn alle virtuele munten aangemaakt bij de lancering door een centrale autoriteit, zoals bij Ripple, ofwel is er sprake van een combinatie van deze twee vormen van creatie. Virtuele valuta lijken dus geen elektronisch geld[157]. Ook volgens de ECB zijn virtuele valuta geen elektronisch geld[158].

Daarnaast is er nog een essentieel verschil. Elektronisch geld heeft immers een duidelijke link met traditioneel geld. De rekeneenheid (euro, dollar …) blijft behouden, wat niet het geval is bij virtuele valuta. Dit heeft een aantal belangrijke consequenties. Zo is er een fluctuerende wisselkoers tussen de virtuele valuta en het traditioneel geld. Prijzen uitgedrukt in bitcoin zullen dus constant aangepast worden in functie van de bitcoin-koers tegenover een referentiemunt. In tegenstelling tot elektronisch geld heb je dus niet de garantie dat je de oorspronkelijke waarde terugkrijgt. Bovendien gebeurt het wisselen van traditioneel geld in virtuele valuta en *vice versa* niet door – sterk gere-

155 Richtlijn 2009/110/EG van het Europees Parlement en de Raad van 16 september 2009 betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronisch geld, tot wijziging van de Richtlijnen 2005/60/EG en 2006/48/EG en tot intrekking van Richtlijn 2000/46/EG, *Pb.L.* 10 oktober 2009, afl. 267, 7.

156 T. Spaas & M. Van Roey, 'Quo vadis Bitcoin?', *Computerrecht* 2015/84, p. 117.

157 Zie in dezelfde zin N. Vandezande, 'Between Bitcoins and mobile payments: will the European Commission's new proposal provide more legal certainty?', *International Journal of Law and Information Technology* 2014, vol. 1, nr. 16, 6; T. Spaas en M. Van Roey, 'Quo vadis Bitcoin?', *Computerrecht* 2015/84, 117.

158 ECB, *Virtual Currency Schemes*, Frankfurt am Main, ECB, 16 november 2015, www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

guleerde – financiële instellingen. Specifieke regulering voor virtuele valuta beperkt zich vooralsnog tot de verplichte uitvoering van de regels voor handelsplatformen en walletaanbieders onder AMLD5 (*infra* 3.13. Overheidsregulering).
Bij *stable coins* (*supra* 3.8. Koersvolatiliteit), namelijk virtuele munten die gekoppeld zijn aan een stabiele waardedrager, zoals bijvoorbeeld de dollar, valt de prijsvolatiliteit grotendeels weg. Indien deze munten evenwel niet zijn uitgegeven door een centrale bank, kredietinstelling of instelling voor elektronisch geld, lijkt het ons niet evident dat ook deze *stable coins* door de ECB economisch gezien gekwalificeerd zouden worden als geld of gekwalificeerd kunnen worden als elektronisch geld onder de Richtlijn Elektronisch geld.

## 3.10. Juridische kwalificatie van virtuele valuta

### 3.10.1. *Ruilovereenkomst, verkoop van een goed of (wettig) betaalmiddel?*

Het lijkt belangrijk om juridisch steeds een onderscheid te maken tussen het aankopen van bitcoins, wat als de aankoop van een goed kan worden beschouwd, en het betalen van een gekocht goed in virtuele valuta zoals bitcoins. Vooral in dat laatste geval speelt de discussie of een bitcoin al dan niet moet worden beschouwd als een betaalmiddel ('geld') of eerder als een ruilmiddel.
Virtuele valuta kunnen in elk geval niet worden beschouwd als een *wettig* betaalmiddel. Niemand is dus verplicht bitcoins of andere virtuele valuta te aanvaarden. Aangezien virtuele valuta vooralsnog juridisch geen wettig betaalmiddel zijn, ontbreken ook juridische garanties zoals de depositobescherming door het Garantiefonds. Vraag is of bitcoins wel een gewoon betaalmiddel zijn. In Nederland heeft in eerste en tweede aanleg al een befaamde Bitcoin-zaak de revue gepasseerd waar de kwalificatie van bitcoin aan de orde was[159].
In een overeenkomst tussen partijen X en Y werd afgesproken dat partij X 2.750 bitcoins koopt van partij Y aan 8,05 euro per bitcoin. Partij X betaalde de volledige koopprijs maar kreeg slechts 990 bitcoins, 1.760 te weinig dus. X heeft de overeenkomst vervolgens buitengerechtelijk partieel ontbonden voor het gedeelte dat Y nog niet was nagekomen. Vervolgens vorderde X voor de rechtbank dat de bitcoin als 'geld' in de zin van afdeling 6.1.11 BW moet worden gezien, waardoor hij zich kon beroepen op artikel 6:125, lid 1 BW, volgens hetwelk de schuldeiser recht heeft op '*vergoeding van de schade die hij heeft geleden doordat na het intreden van het verzuim de koers van het geld tot betaling waarvan de verbintenis strekt, zich ten opzichte van die van het geld van een of meer andere landen heeft gewijzigd*'. Hij vorderde dus schadevergoeding *in natura* door de levering door Y aan X van 1.760 bitcoins of bij niet-nakoming een geldelijke

159 Zie voor een zaak over de kwalificatie van de virtuele valuta ether: W. Weij & M.C. Landerbarthol, 'Ruis in de ether en de juridische kwalificatie(s) van cryptovaluta' (noot bij Rb. Midden-Nederland 7 december 2017, ECLI:NL:RBMNE:2017:66461), *Tijdschrift voor Internetrecht* 2018/2. Volgens de rechtbank is ether een 'goed', zodat een dwangsom kan worden opgelegd met betrekking tot het overmaken van ethers.

schadevergoeding ter waarde van de actuele waarde van de bitcoins, namelijk 132.792 euro, gelet op de enorme waardestijging van 836,71%.

Op basis van de parlementaire geschiedenis van artikel 6:112 BW, volgens welke het 'geld' betaald ter voldoening van een verbintenis gangbaar moet zijn in het land waar de betaling geschiedt, besloot de rechtbank in eerste aanleg[160] dat een bitcoin niet juridisch als 'geld' kon worden gekwalificeerd, maar moet worden gezien als een *ruilmiddel*. Dit is op zichzelf juist: bitcoins zijn op dit moment duidelijk niet gangbaar in de zin van artikel 6:112 BW en daarom op dit moment ook geen geld in de zin van deze bepaling.[161] De rechtbank overwoog echter verder – minder juist – dat het om een 'wettig betaalmiddel' moet gaan om juridisch als geld gekwalificeerd te worden. Op basis van artikelen 10 en 11 Verordening EG nr. 974/98 is alleen de euro een 'wettig betaalmiddel' in de deelnemende lidstaten, aldus de rechtbank.[162] Volgens de rechter is de schade die voor vergoeding in aanmerking komt, de schade die X heeft geleden van het sluiten van de overeenkomst tot het moment van partiële ontbinding van de overeenkomst. In deze periode is de koers van de bitcoin met 1 euro gestegen, waardoor de schade 1.760 euro bedraagt.

In tweede aanleg deed vervolgens het Hof Arnhem-Leeuwarden uitspraak op 31 mei 2016[163]. Volgens het hof kan in deze zaak geen beroep worden gedaan op artikel 6:125 BW, maar om een andere overweging dan de rechtbank. Volgens het hof heeft het artikel immers geen betrekking op waardeschommelingen van gekochte goederen die niet zijn geleverd, maar heeft het betrekking op een situatie waarin schade wordt geleden door een te late betaling. Door de partiële ontbinding is de betalingsverplichting van de bitcoins echter vervallen, waardoor volgens het hof de overeenkomst niet meer met vertraging kan worden nagekomen en van schade door een koersverschil op het moment van de dagvaarding geen sprake kan zijn. Hierdoor onderzoekt het hof niet of de bitcoin juridisch als 'geld' moet worden beschouwd. Het hof kwalificeert bitcoin echter als een *goed* en een '*gekochte zaak*' in de zin van artikel 7:36 BW. Volgens dat laatste artikel moet de schade van X worden begroot op 1.760 euro, namelijk de waardestijging van de bitcoin tussen het sluiten van de koopovereenkomst en de partiële ontbinding ervan.

Fiscaal gezien wordt er anders gekeken naar virtuele valuta. In het arrest-*Hedqvist* van het Hof van Justitie van de Europese Unie van 22 oktober 2015 was de vraag aan de orde of er btw moet worden betaald op bitcoin[164]. Het HvJEU besliste immers dat bitcoin geen 'lichamelijke zaak' is zoals bepaald in artikel 14 Btw-richtlijn[165]. Bitcoin dient

160 Rb. Overijssel 14 mei 2015, ECLI:NL:RBOVE:2014:2667.

161 P. Rank, 'Betaling in bitcoins: geld of ruilmiddel, betaling of inbetalinggeving?', *Ars Aequi* 2015, p. 177-185.

162 Zie kritisch hierover W.F. Dammers, 'Bitcoins: een vreemde zaak?' (noot bij Hof Arnhem-Leeuwarden 31 mei 2016), *Tijdschrift voor Internetrecht* 2016, p. 112.

163 Hof Arnhem-Leeuwarden 31 mei 2016, ECLI:NL:GHARL:2016:4219, met noot van F. Dammers, 'Bitcoins: een vreemde zaak?', *Tijdschrift voor Internetrecht*, p. 110-112.

164 HvJ 22 oktober 2015, nr. C-264/14, *Hedqvist*. W.F. Dammers, 'Bitcoins: een vreemde zaak?' (noot bij Hof Arnhem-Leeuwarden 31 mei 2016), *Tijdschrift voor Internetrecht* 2016, p. 111.

165 Richtlijn 2006/112/EG van de Raad van 28 november 2006 betreffende het gemeenschappelijke stelsel van belasting over de toegevoegde waarde, *Pb.L.* 11 december 2006/347, p. 1.

volgens het hof immers geen ander doel dan een gebruik als betaalmiddel. Volgen het hof kan de omwisseling van bitcoins in traditionele valuta dientengevolge niet worden gekwalificeerd als een levering van goederen in de zin van artikel 14 Btw-richtlijn. Het Hof Arnhem-Leeuwarden kwalificeerde een bitcoin evenwel toch als een goed en een gekochte zaak. Hoewel een bitcoin geen 'wettig betaalmiddel' is, blijft de vraag bediscussieerbaar of een bitcoin al dan niet als gangbaar betaalmiddel gekwalificeerd zou moeten worden. Het is in dezen interessant om erop te wijzen dat de advocaat-generaal in zijn conclusie bij de *Hedqvist*-zaak bitcoins aanmerkt als een betaalmiddel maar niet als een wettig betaalmiddel. De advocaat-generaal stelt dat bitcoins vanuit btw-oogpunt dezelfde functie vervullen als wettige betaalmiddelen en bijgevolg volgens het beginsel van fiscale neutraliteit, als uitdrukking van het beginsel van gelijke behandeling, in beginsel gelijk behandeld moeten worden als een wettig betaalmiddel in het kader van de Btw-richtlijn[166].

Volgens de Vijfde Anti-witwasrichtlijn[167] is een virtuele valuta de digitale weergave van waarde die niet door een centrale bank of een overheid wordt uitgegeven of gegarandeerd, die niet noodzakelijk aan een wettelijk vastgestelde valuta is gekoppeld en die niet de juridische status van valuta of geld heeft, maar die door natuurlijke of rechtspersonen als ruilmiddel wordt aanvaard en die elektronisch kan worden overgedragen, opgeslagen en verhandeld. Volgens de Richtlijn mogen virtuele valuta niet worden verward met elektronisch geld zoals gedefinieerd in artikel 2, punt 2 Richtlijn 2009/110/EG, noch met het ruimere begrip 'geldmiddelen' zoals gedefinieerd in artikel 4, punt 25 EU-Richtlijn nr. 2015/2366[168], noch met monetaire waarde die is opgeslagen op instrumenten die zijn vrijgesteld als gespecificeerd in artikel 3, k) en l) EU-Richtlijn nr. 2015/2366, noch met speelgeld dat alleen binnen een specifieke spelomgeving kan worden gebruikt. Hoewel virtuele valuta vaak als betaalmiddel kunnen worden gebruikt, zouden zij ook voor andere doeleinden kunnen worden gebruikt en ruimere toepassingen vinden, bijvoorbeeld als ruilmiddel, belegging, om waarde op te slaan of voor gebruik in onlinecasino's. De Vijfde Anti-witwasrichtlijn omvat alle gebruiksmogelijkheden van virtuele valuta. Lokale of zogenaamde 'complementaire' valuta die worden gebruikt door een klein aantal gebruikers in een zeer beperkt netwerk zoals een stad of een regio, worden evenwel niet als virtuele valuta beschouwd.

Dat de regels voor btw en antiwitwassen virtuele valuta wel op één lijn stellen met wettig betaalmiddel is begrijpelijk. Om witwassen tegen te gaan, wil de overheid alles wat ruilwaarde heeft onder deze regels brengen, ook al zou het om postzegels of edelstenen gaan. Voor btw moet ook handel in buitenlandse valuta op dezelfde wijze worden be-

166 HvJ 22 oktober 2015, nr. C-264/14, *Hedqvist*, concl. Adv. Gen. J. Kokott.

167 Richtlijn 2018/843 van het Europees Parlement en de raad van 30 mei 2018 tot wijziging van Richtlijn 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU, *Pb.L.* 19 juni 2018/156, p. 43.

168 Richtlijn 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG, *Pb.L.* 23 december 2015/337, p. 35.

handeld als Nederlandse valuta, hoewel buitenlandse valuta niet als geld telt in Nederland. In het Burgerlijk Wetboek gaat het evenwel vooral om de vraag of burgers verplicht zijn bepaalde ruilmiddelen die als 'geld' tellen te aanvaarden. Op dit moment mag niemand worden gedwongen om tegen zijn wil een koopprijs of salaris in bitcoin te accepteren. De andere regels over 'geld' in het BW hangen hiermee samen.
Het is tevens nog een interessante discussie of bitcoins kunnen vallen onder 'digitale inhoud' zoals bepaald in de richtlijn consumentenrechten[169]. Hieronder vallen namelijk '*gegevens die in digitale vorm geproduceerd en geleverd worden […] ongeacht of de toegang tot deze gegevens wordt verkregen […] vanaf een materiële drager of langs een andere weg*'. Overeenkomsten met betrekking tot de levering van digitale inhoud vallen per definitie onder het toepassingsgebied van de richtlijn. Indien bitcoins kunnen worden aangemerkt als dergelijke 'digitale inhoud', heeft de consument een herroepingsrecht en moet de verkoper voldoen aan verregaande informatieverplichtingen[170].

### 3.10.2. *Fiscaal*

In de *Hedqvist*-zaak stelt het Hof van Justitie van de Europese Unie dat '*diensten zoals die aan de orde in het hoofdgeding – die bestaan in het inwisselen van traditionele valuta's tegen eenheden van de virtuele valuta „bitcoin" en omgekeerd, die worden verricht tegen betaling van een bedrag dat overeenkomt met de marge die ontstaat uit het verschil tussen de prijs waarvoor de betrokken marktdeelnemer de valuta koopt en de prijs waarvoor hij deze verkoopt aan zijn klanten –, van de btw vrijgestelde handelingen vormen in de zin van deze bepaling.*'[171] Het HvJEU argumenteert dat handelingen met betrekking tot niet-traditionele valuta, namelijk andere valuta dan degene die in één of meerdere landen het wettelijke betaalmiddel zijn en als enige doel hebben om als betaalmiddel te worden gebruikt, financiële handelingen zijn in de zin van de Btw-richtlijn, wat een bijkomede reden is om het inwisselen van bitcoins tegen traditionele valuta vrij te stellen van btw.
De ruling 2017.852[172] van 5 december 2017 van de Dienst voorafgaande beslissingen stelt dat er – in dit geval op zijn minst – belasting betaald moet worden over de meerwaarde op de verkoop van virtuele valuta als een divers inkomen ingevolge artikel 90, 1° WIB 1992. Een student ontwikkelde voor zijn studies een applicatie voor automatische aan- en verkoop van bitcoins. Volgens de fiscus gaat het *in casu* om speculatie en niet om winst uit gewone meerwaarde. De activiteiten van de student waren onvoldoende gestructureerd om te kunnen gelden als beroepsinkomen. Het gaat dus om een particulier die meerwaarde genereert uit speculatie. Daarom valt het inkomen in de

169 Richtlijn 2011/83/EU van het Europees Parlement en de Raad van 25 oktober 2011 betreffende consumentenrechten.
170 Volgens Dammers kunnen bitcoins aangemerkt worden als digitale inhoud zoals bepaald door de richtlijn. Zie W.F. Dammers, 'Bitcoins: een vreemde zaak?' (noot bij Hof Arnhem-Leeuwarden 31 mei 2016), *Tijdschrift voor Internetrecht* 2016, p. 113.
171 HvJ 22 oktober 2015, nr. C-264/14, *Hedqvist*.
172 FOD Financiën – Dienst voorafgaande beslissingen, 'News – Nr. 3', www.ruling.be/sites/default/files/content/download/files/nieuwsbrief_dvb_3_nl.pdf.

categorie *divers inkomen* en wordt het belast aan 33% (art. 90, 1° WIB 1992). Daar komen nog de gemeentelijke opcentiemen bij. Stel dat een particulier zijn bitcoins als een goede huisvader beheerde, zoals bij aandelen die men lange tijd aanhoudt, dan zou dit in beginsel kunnen vallen onder het normale beheer van het privévermogen, wat belastingvrij is. Indien een professional echter meerwaarde genereert uit het verhandelen van virtuele valuta, valt dit onder het beroepsinkomen, wat progressief belast wordt en onderhevig is aan sociale bijdragen. De vraag is natuurlijk in welk geval speculatieve activa zoals virtuele munten als een goede huisvader beheerd kunnen worden. Hoewel de Dienst voorafgaande beslissingen steeds geval per geval beoordeelt, is hij op basis van de ingediende *prefilings* en aanvragen van oordeel dat beleggingen in virtuele munten meestal een speculatief karakter hebben en de inkomsten uit die beleggingen bijgevolg diverse inkomsten vormen overeenkomstig artikel 90, 1° WIB 1992 of beroepsinkomsten in het geval van een beroepswerkzaamheid.
In Nederland stelt de Belastingdienst dat cryptovaluta, zoals bitcoins en andere virtuele betaalmiddelen, voor de inkomstenbelasting onder 'overige bezittingen' in box 3 vallen[173]. De waarde van virtuele munten is immers een onderdeel van het totale vermogen. Indien dat meer is dan 30.000 euro[174], betaal je vervolgens in 2020 – afhankelijk van de hoogte van het vermogen – tussen de 0,54 en 1,60% belasting[175]. Het is natuurlijk aan de houder van virtuele valuta om deze aan te geven. Indien je beslist om dit niet te doen, houdt dit een risico in. De blockchain waarop alle transacties geregistreerd staan, vergeet immers niets en vaak kennen de handelsplatformen je identiteit. In de Verenigde Staten heeft de federale belastingdienst, de IRS, van de rechter[176] met succes van het handelsplatform *Coinbase* kunnen vorderen om de identiteit van meer dan 14.000 rekeningen te identificeren, namelijk rekeningen met transacties boven de 20.000 dollar, samen goed voor bijna 9 miljoen transacties[177].

## 3.11. Veiligheid en risico

De veiligheid van systemen voor virtuele valuta hangt af van heel wat aspecten[178]. Deze sectie gaat kort in op enkele aspecten.
Virtuele munten die gebruikmaken van *Proof of Work* (PoW, *supra* 3.5. Ecologische impact), zoals bijvoorbeeld Bitcoin, veronderstellen dat er nooit een participant of een groep samenwerkende participanten meer dan 50% van de rekenkracht zal bezitten, omdat deze entiteit dan in staat is om de blockchain te herschrijven en oudere transacties ongedaan te maken. In 2018 kreeg onder meer *Bitcoin Gold* een dergelijke aanval

173 https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/prive/vermogen_en_aanmerkelijk_belang/vermogen/wat_zijn_uw_bezittingen_en_schulden/uw_bezittingen/overige_bezittingen/.
174 Art. 5.5 WIB.
175 www.homefinance.nl/belastingen/inkomstenbelasting-box-3.asp.
176 US District Court Northern District of California 28 november 2017, nr. 17-cv-01431-JSC, *US/Coinbase*.
177 J.J. Roberts, 'IRS Wins Bitcoin Fight, Gets Access to 14,000 Coinbase Accounts', *Fortune*, 30 november 2017, http://fortune.com/2017/11/29/irs-coinbase.
178 Zie algemeen X. Li, P. Jiang, T. Chen, X. Luo & Q. Wen, 'A survey on the security of blockchain systems', *Future Generation Computer Systems* 2017.

te verduren. De aanvaller heeft daarmee naar schatting 18 miljoen dollar buitgemaakt van *Bitcoin Gold*-handelsplatformen[179]. Een concrete bezorgdheid in dit opzicht is dat momenteel naar schatting 70 tot 80% van de delfcapaciteit gecontroleerd wordt door Chinese bedrijven. De Chinese overheid – die allesbehalve positief staat tegenover virtueel geld buiten haar controle – kan in beginsel de waarde van bitcoin kelderen door deze bedrijven te dwingen samen te werken. Daarnaast resulteert een dalende koers op termijn in lagere veiligheid. In een dergelijke context zullen delvers hun activiteiten immers afbouwen wegens onvoldoende rendabel of verlieslatend, waardoor dergelijke aanval waarschijnlijker wordt. De mate van veiligheid van een open blockchainnetwerk gebaseerd op *PoW* is dus variabel en volgt de waarde van de virtuele munt.

Een op dit moment meer theoretische bedenking betreft de cryptografische bouwblokken (digitale handtekeningen en hashfuncties), waarvan de veiligheid op lange termijn niet gegarandeerd is. Kwantumcomputers worden hierbij gezien als de meest pertinente dreiging. Daarom wordt onder meer gewerkt aan blockchaintechnologieën die gebruikmaken van kwantumresistente cryptografie of zelfs direct van principes uit de kwantummechanica[180].

Elke participant in een blockchainnetwerk maakt bovendien gebruik van software. Die software kan natuurlijk fouten (*bugs*) bevatten. Daarvan zijn diverse voorbeelden zoals Zcoin in 2017[181], Bitcoin in 2013[182] en EOS in 2018[183, 184]. Bovendien kan zelfs de hardware fouten bevatten. Onderzoekers aan de Vlaamse KU Leuven ontdekten onder andere een kwetsbaarheid in Intels SGX, een sterk beveiligde kluis in de processor. Geplande virtuele munten zoals *MobileCoin* zullen evenwel intensief gebruikmaken van deze kluis[185]. *Bugs* kunnen dramatische gevolgen hebben en kunnen onmogelijk uitgesloten worden.

Een volgend probleem betreft de private sleutel van gebruikers. In de oorspronkelijke opzet heeft elke participant in het netwerk van de virtuele munt een eigen geheime cryptografische sleutel, die je kunt zien als een lang wachtwoord. Indien een persoon zijn geheime sleutel verliest[186], is hij niet langer in staat om zijn virtuele munten te transfereren waardoor deze bevroren blijven op de blockchain. Heel wat mensen heb-

179 J.J. Roberts, 'Bitcoin Spinoff Hacked in Rare '51% Attack', *Fortune*, 29 mei 2018, http://fortune.com/2018/05/29/bitcoin-gold-hack.

180 Zie 'If quantum computers threaten blockchains, quantum blockchains could be the defense', *MIT Technology Review*, 1 mei 2018, www.technologyreview.com/s/611022/if-quantum-computers-threaten-blockchains-quantum-blockchains-could-be-the-defense.

181 P. Insom, 'Zcoin's Zerocoin bug explained in detail', *Zcoin*, 21 februari 2017, https://zcoin.io/zcoins-zerocoin-bug-explained-in-detail.

182 V. Buterin, 'Bitcoin Network Shaken by Blockchain Fork', *Bitcoin Magazine*, 12 maart 2013, https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448.

183 N. Varshney, 'The EOS mainnet nightmare: How not to launch a blockchain network', *The Next Web*, 8 juni 2018, https://thenextweb.com/hardfork/2018/06/08/eos-mainnet-nightmare.

184 N. Varshney, 'Researchers continue to find vulnerabilities in $9 billion cryptocurrency EOS', *The Next Web*, 14 juni 2018, https://thenextweb.com/hardfork/2018/06/14/eos-cryptocurrency-bugs.

185 A. Hertig, 'What Intel's Foreshadow Flaw Means for the Future of Cryptocurrency', *Coindesk*, 16 augustus 2018, www.coindesk.com/what-intels-foreshadow-flaw-means-for-the-future-of-cryptocurrency.

186 Zie H. De Vauplane, 'Blockchain and conflicts of law', *RTDF* 2017/4, p. 50.

ben zo al virtuele munten verloren. Volgens een schatting[187] zou zo al bijna vier miljoen aan bitcoins onherroepelijk verloren gegaan zijn[188]. Zo is er het verhaal van de Britse informaticus James Howell, die een harde schijf weggegooid heeft met daarop de sleutel die hem toegang gaf tot 7.500 bitcoins. Ook wanneer iemand komt te overlijden, is er een risico dat de nabestaanden geen weet hebben van de virtuele munten van de overledene, of dat ze er geen toegang tot kunnen krijgen (bijvoorbeeld omdat de private sleutel met een sterk wachtwoord beveiligd is). In tegenstelling tot traditionele systemen zijn er geen vangnetten en is het de eindgebruiker zelf die verantwoordelijk is voor de bescherming van zijn cryptografische sleutel en dus zijn bitcoins.

Velen bewaren hun virtueel geld bovendien in onlineportefeuilles (*wallets*) die beheerd worden door – doorgaans buitenlandse– bedrijven. De Nederlandse bank ING werkt ondertussen ook aan een systeem om veilig virtueel geld van haar klanten te beheren. ABM AMRO en Rabobank waren van eveneens van plan onlineportefeuilles aan te bieden, maar stapten af van het idee wegens te riskant[189]. Het concept van beheerde onlineportefeuilles gaat natuurlijk in tegen de oorspronkelijke Bitcoin-filosofie van een gedistribueerd netwerk, aangezien men toch opnieuw heel wat vertrouwen moet stellen in deze bedrijven, die zelfs de banken kunnen zijn die Bitcoin net overbodig wou maken.

De veiligheid van beheerde onlineportefeuilles is niet altijd even afdoende. Het meest beruchte is Mt. Gox[190], waarbij 850.000 bitcoins gestolen werden. Hoewel er later 200.000 werden teruggevonden, ging Mt. Gox failliet in 2014. De gedupeerden ondernamen juridische stappen[191]. In januari 2018, werd Coincheck gehackt[192], waarbij ongeveer 500 miljoen NEM-virtuele munten gestolen werden. Omgerekend bedroeg de buit ongeveer 530 miljoen dollar. Er is ondertussen een hele lijst van gehackte handelsplatformen en aanbieders van onlinewallets[193]. Ook in 2019 werden vonden verschillende diefstallen van virtueel geld bij walletbeheerders plaats, vaak voor miljoenen uitgedrukt in dollars: Cryptopia ($2,44 miljoen), Binance ($41 miljoen), LocalBitcoins ($27 000), Bithumb ($19 miljoen), Gatehub ($10 miljoen), BitTrue ($5 miljoen) en BitPoint ($32 miljoen)[194].

---

187 J.J. Roberts, 'Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says', *Fortune*, 25 november 2017, http://fortune.com/2017/11/25/lost-bitcoins.

188 Op dit moment zijn er ongeveer 17 miljoen bitcoins in omloop en volgens de Bitcoin-regels zullen er maximum 21 miljoen gecreëerd worden.

189 W. Simons, 'ABN AMRO en Rabobank laten bitcoin (BTC) handel in 2020 links liggen', *Bitcoin Magazine NL*, 17 december 2019, https://bitcoinmagazine.nl/2019/12/abn-rabo-bitcoin-2020/.

190 J.L. Trautman, 'Virtual currencies – Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?', *Richmond Journal of Law and Technology* 2014.

191 W. Zhao, 'Mt. Gox Creditors Are Preparing to Claim for Bitcoin Repayments', *Coindesk*, 3 augustus 2018, www.coindesk.com/mt-gox-creditors-are-preparing-to-claim-for-bitcoin-repayments.

192 D. Pollock, 'Story of Coincheck: How to Rebound After the 'Biggest Theft in the History of the World', *CoinTelegraph*, 3 april 2018, https://cointelegraph.com/news/story-of-coincheck-how-to-rebound-after-the-biggest-theft-in-the-history-of-the-world.

193 A. Munkachy, 'The Complete List of Cryptocurrency Exchange Hacks – 30+ Hacks', *CoinIQ*, 21 juni 2018, https://coiniq.com/cryptocurrency-exchange-hacks.

194 R. Pompon, S. Vinerg, *Cryptocurrency Hacks 2019*, F5 Labs, 11 september 2019, https://www.f5.com/labs/articles/threat-intelligence/cryptocurrency-hacks-2019.

Bovendien werden ook al individuele onlineportefeuilles gehackt waarbij niet het onlineplatform maar de eigenaar van het virtueel geld aangevallen werd. Via een zogenaamde *SIM swap attack* werd zo begin 2018 het telefoonnummer van een investeerder in virtueel geld gestolen. Via deze weg kregen de hackers toegang tot de onlineportefeuille van de investeerder, die aldus 1.500 bitcoins verloren is[195]. Een dergelijke aanval heeft op zich niets te maken met blockchaintechnologie of virtueel geld. Ook de officiële Twitteraccount van Twitter stichter en CEO Jack Dorsey werd op een gelijkaardige manier gehackt. Zelfs als de blockchain of de virtuele munt zelf perfect veilig zou zijn, bestaat er nog steeds allerlei IT-infrastructuur errond die gevoelig blijft voor hackpogingen.

Het voordeel van blockchain is wel dat alles traceerbaar is. We kunnen exact zien welke weg de gestolen virtuele valuta afgelegd hebben. Indien de dief bijvoorbeeld op een handelsplatform zijn virtuele valuta inwisselt voor dollars of euro's loopt hij of zij het risico tegen de lamp te lopen. In het geval van de Coincheck-hack zijn de gestolen virtuele valuta gelinkt aan een account op een handelsplatform in Vancouver, Canada[196]. Desondanks kan de transactiegeschiedenis van virtueel geld gecamoufleerd worden door gebruik te maken van *mixing services* of *tumblers*[197]. Bovendien zijn er virtuele munten die trachten de privacy van de gebruiker beter te beschermen. Zo zijn er *Zcash* en *Bitcoin Private* die gebruikmaken van geavanceerde cryptografie. Uit een transactie kun je niet afleiden van welk pseudoniem de virtuele munten afkomstig zijn, naar waar ze getransfereerd worden en hoeveel er getransfereerd wordt. Traceren wordt in zulke situatie uitermate moeilijk.
Dergelijke *hacks* maken de noodzaak aan regulering en toezicht wenselijk ter bescherming van gebruikers. Daarbij kunnen enerzijds handelsplatformen verplicht worden de identiteit van de rekeninghouders met voldoende hoge zekerheid vast te stellen door middel van een zogenaamde KYC (*know your customer*)-procedure, zoals bij banken. Ten tweede kunnen sterke veiligheidsmaatregelen verplicht worden, waarbij geregelde audits nagaan of hieraan voldaan is. Ten derde kunnen kapitaals- en continuïteitsvereisten opgelegd worden. Ten slotte zou het geregistreerde handelsplatformen verboden kunnen worden om moeilijk te traceren virtuele munten te verhandelen.

## 3.12. **Zelfregulering**

In gedistribueerde blockchainnetwerken zijn een hele set regels van toepassing die tal van vragen beantwoorden. Hoe groot mag een blok zijn? Hoe wordt de moeilijkheids-

195 B. Winck, 'One cryptocurrency investor reportedly lost $24 million worth of bitcoin in a SIM swap attack', *Business Insider*, 11 november 2019, https://markets.businessinsider.com/currencies/news/bitcoin-investor-loses-24-million-of-crypto-sim-swap-hackers-2019-11-1028677818.

196 M.J. Zuckerman, 'Stolen Coincheck NEM Found In Exchanges In Canada, Japan, Law Enforcement To Be Informed', *CoinTelegraph*, 2 maart 2018, https://cointelegraph.com/news/stolen-coincheck-nem-found-in-exchanges-in-canada-japan-law-enforcement-to-be-informed.

197 U.W. Chohan, *The Cryptocurrency Tumblers: Risks, Legality and Oversight*, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080361.

graad van een cryptografische puzzel bepaald? Hoeveel en hoe snel komen nieuwe munten in omloop? Deze regels worden collectief door het netwerk afgedwongen. Wie bepaalt echter deze regels en hoe gaat dit afdwingen in zijn werk? Laat ons even kijken naar Bitcoin als voorbeeld.

Elke participant in het netwerk downloadt de Bitcoin-software en voert die uit. Deze software bevat de toepasselijke regels. Van tijd tot tijd wordt een nieuwe versie van die software gepubliceerd, met mogelijks gewijzigde regels. Binnen de Bitcoin-gemeenschap (*community*) is heel wat discussie op basis waarvan het Bitcoin-*core team*, de (niet-verkozen) leiding van de Bitcoin-softwareontwikkelaars, een nieuwe versie voorstelt. Het uitvoeren van deze regels gebeurt vervolgens door de delvers. Zij creëren aan een bepaalde doelfrequentie nieuwe blokken die op het netwerk verspreid worden. Elk blok, alsook de daarin vervatte transacties, moeten aan de afgesproken regels voldoen. Het verifiëren of dit het geval is, gebeurt door de *full nodes*, namelijk de participanten met een volledige kopie van de blockchain. Indien een *full node* een blok ontvangt dat niet aan de regels voldoet, zal het dit blok niet aan haar lokale blockchainkopie toevoegen en niet verder op het netwerk verspreiden. Een blok dat niet aan de regels voldoet, zal dus snel door het netwerk verworpen worden. In het Bitcoin-netwerk controleert een handvol bedrijven het leeuwendeel van de delfcapaciteit, terwijl er een paar duizend *full nodes* zijn. Enkel de delvers krijgen een vergoeding voor hun werk. De identificatie van dit zogenaamde Bitcoin-core team en de andere softwareontwikkelaars, zou van belang kunnen zijn in de zoektocht naar dragers van aansprakelijkheid. In de praktijk zijn deze softwareontwikkelaars evenwel moeilijk te identificeren, aangezien zij ervoor kunnen opteren om onder een pseudoniem te werken. Het is tevens een bijkomende complicatie dat een groep zich kan afsplitsen indien zij het ergens niet mee eens zijn. De identiteit van de bedenker van Bitcoin is nog steeds onbekend, maar maakt geen deel meer uit van het core team. Het core team verandert dus gedurende de tijd.

Samengevat is er een vorm van zelfregulering door het Bitcoin-netwerk, gebaseerd op consensus. Wanneer een deel van de participanten niet langer akkoord gaat met de regels, splitsen ze zich af, zoals we al gezien hebben (*supra* 3.4. Het nieuwe goud?), en ontstaat aldus een nieuwe virtuele munt, met zijn eigen regels, consensus, delfcapaciteit en koers.

In tegenstelling tot meer gedistribueerde virtuele munten, zoals Bitcoin en Litecoin, zijn er ook meer gecentraliseerde virtuele munten. De bekendste is XRP op het Ripplenetwerk, dat door Ripple Labs ontwikkeld werd en in 2012 gelanceerd werd. XRP focust op internationale transacties tussen banken, hoewel het ook buiten die context wordt gebruikt. XRP is op het moment van schrijven de derde grootste virtuele munt qua marktkapitalisatie. Ripple Labs ontwikkelt de software en het netwerk wordt veilig gehouden door een beperkt aantal door Ripple Labs erkende bedrijven en organisaties wereldwijd, waaronder MIT, Santander, Telindus en TU Delft. Regelmatig worden door Ripple Labs nieuwe validatoren aan het netwerk toegevoegd. De kans op een *split* is in zulk model uiteraard veel kleiner. Tegenover deze minder gedistribueerde benadering staan een aantal belangrijke voordelen. De transactiekosten liggen ten eerste

een stuk lager: op het moment van schrijven was dit minder dan 0,04 dollarcent[198], beduidend lager dus dan ongeveer 0,5 dollar voor Bitcoin. Ripple Labs claimt bovendien een capaciteit van 1.500 transacties per seconde, alsook de mogelijkheid om tot 50.000 transacties per seconde te schalen, terwijl Bitcoin er maar een tiental aankan. Transacties zouden binnen de vier seconden verwerkt worden[199], terwijl dit op blockchain tot een uur kan duren. Ten slotte zijn er geen energieverslindende rekencentra vereist. Dit lijkt dan ook meer dan Bitcoin een realistische uitdager voor Swift[200].
Ripple krijgt echter ook kritiek te verduren. In Ripple worden virtuele munten namelijk niet gedolven. Alle XRP-munten bestaan sinds de lancering van Ripple. Dit zorgt ervoor dat de rijkdom nog meer geconcentreerd is dan bij Bitcoin[201]. Alle 100 miljoen munten bestaan immers sinds de lancering van Ripple in 2012 en een vijfde daarvan hielden de makers voor zichzelf[202]. Het bespreken van deze kwestie valt echter voor de rest buiten de reikwijdte van dit boek.

## 3.13. **Overheidsregulering**

Het netwerk van een virtuele munt bestaat al snel uit duizenden participanten verspreid over de hele wereld. Voor een individuele staat is het bijgevolg bijna onmogelijk om een dergelijk netwerk, zonder centrale partij, aan banden te leggen of te reguleren. Toch kunnen de handelsplatformen waar virtuele valuta omgezet worden in fiduciair geld zoals de euro, alsook de beheerders van onlineportefeuilles voor virtuele munten (*wallets*), wel gemakkelijker gereguleerd worden (en gemakkelijker geïdentificeerd worden als mogelijke aansprakelijke actoren).
De Europese Unie heeft daarom in april 2018 de Vijfde Anti-witwasrichtlijn goedgekeurd[203]. Het is de bedoeling dat lidstaten zowel handelsplatformen van virtuele munten als walletbeheerders[204] onder de AML/CFT-regeling (Anti-Money Laundering/Combating the Financing of Terrorism) brengen[205]. Tegen 10 januari 2020 moesten de lidstaten wetgeving aannemen om handelsplatformen en walletaanbieders te registre-

198 https://bitinfocharts.com.
199 https://ripple.com/xrp.
200 M. Arnold, 'Ripple and Swift slug it out over cross-border payments', *Financial Times*, 6 juni 2018, www.ft.com/content/631af8cc-47cc-11e8-8c77-ff51caedcde6.
201 L. Shin, 'Meet The Crypto Billionaires Getting Rich From Ripple's XRP', *Forbes*, 2 januari 2018, www.forbes.com/sites/laurashin/2018/01/02/meet-the-crypto-billionaires-getting-rich-from-ripples-xrp.
202 M. Orcutt, 'No, Ripple Isn't the Next Bitcoin', *MIT Technology Review*, 11 januari 2018, www.technologyreview.com/s/609958/no-ripple-isnt-the-next-bitcoin.
203 Richtlijn 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU, *Pb.L.* 19 juni 2018/156, p. 43.
204 De Richtlijn noemt een walletbeheerder een 'aanbieder van een bewaarportemonnee' en definieert deze als '*een entiteit die diensten aanbiedt om namens haar cliënten cryptografische privésleutels te beveiligen om virtuele valuta aan te houden, op te slaan en over te dragen*'.
205 T. Keatinge, D. Carlisle & F. Keen, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, European Union, 2018, www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604970.

ren. Dit wordt beschouwd als een belangrijke en noodzakelijke eerste stap om transparantie te brengen in de netwerken van virtuele munten. De richtlijn is echter niet van toepassing op handelsplatformen die enkel toelaten om virtuele munten in te wisselen tegen andere virtuele munten (enkel het inwisselen van virtuele valuta voor fiduciair geld en omgekeerd), wat in een van de volgende stappen zou gebeuren. Het is de bedoeling dat hun klanten geïdentificeerd worden en de handelsplatformen verplicht worden verdachte activiteiten te melden[206]. Het blijft echter mogelijk om virtuele munten te verhandelen buiten een handelsplatform om. Ook is het mogelijk om zelf virtuele munten te delven, wat evenwel omslachtiger en voor vele virtuele munten erg energie-intensief is.

In Nederland is op het moment van schrijven (februari 2020) de uitvoering van de richtlijn in het voorstel Implementatiewet wijziging vierde anti-witwasrichtlijn echter nog steeds in behandeling bij de Eerste Kamer. Het wetsvoorstel bevat voornamelijk wijzigingen van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Met dit wetsvoorstel dienen aanbieders van diensten voor het wisselen tussen virtuele valuta en fiat valuta en aanbieders van bewaarportemonnees zich te registreren bij De Nederlandsche Bank (het voorstel van een vergunningenstelsel is ondertussen verlaten) en worden ze onder de reikwijdte van de Wwft gebracht waarvan ze de algemene vereisten dus moeten naleven. Dat betekent onder andere dat zij onderzoek moeten doen naar hun cliënten en ongebruikelijke transacties dienen te melden bij de Financiële Inlichtingen Eenheid (FIU). Aangezien de parlementaire behandeling meer tijd in beslag neemt, geldt de registratieplicht en vereiste tot naleving van de algemene vereisten van de Wwft dus nog niet vanaf 10 januari 2020.

We zien momenteel wereldwijd zeer uiteenlopende benaderingen door overheden met betrekking tot de nieuwe realiteit van virtuele munten. Dit gaat van een zeer soepel en ondersteunend beleid, zoals in Zwitserland[207], tot een erg restrictief beleid, zoals in China[208, 209], hoewel China desondanks algemeen echter wel positief staat tegenover blockchain als technologie voor organisaties en bedrijven. Christine Lagarde, (voormalige) managing director van het IMF, stelde in maart 2018 het volgende: '*To be truly effective, all these efforts require close international cooperation. Since crypto-assets know no borders, the framework to regulate them must be global as well*'[210]. Er wacht dus een grote uitdaging op dit vlak.

206 European Commission, 'Statement By First Vice-President Timmermans, Vice-President Dombrovskis and Commissioner Jourovà on the adoption by the European Parliament of the 5th Anti-Money Laundering Directive', 19 april 2018, http://europa.eu/rapid/press-release_STATEMENT-18-3429_en.htm.

207 R. Atkins, 'Switzerland sets out guidelines to support initial coin offerings', *Financial Times*, 16 februari 2018, www.ft.com/content/52820f90-1307-11e8-940e-08320fc2a277.

208 S. Ehrlich, 'Making Sense Of China's Grand Blockchain Strategy', *Forbes*, 17 september 2018, www.forbes.com/sites/stevenehrlich/2018/09/17/making-sense-of-chinas-grand-blockchain-strategy.

209 J. Brett, 'China's Dichotomy Between Cryptocurrency And Blockchain', *Forbes*, 30 december 2019, https://www.forbes.com/sites/jasonbrett/2020/12/30/chinas-dichotomy-between-cryptocurrency-and-blockchain/.

210 C. Lagarde, 'Addressing the Dark Side of the Crypto World', *IMF Blog*, 13 maart 2018, https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world.

## 3.14. Initial Coin Offerings

### 3.14.1. *Algemeen*

Als een bedrijf op een traditionele manier een IT-dienst aanbiedt, maakt het gebruik van een centrale dienst waar het controle over heeft. Denk aan Facebook, Google Search, Dropbox, eBay, Uber en vele andere diensten. In zulk geval zijn er diverse manieren om inkomsten te genereren: aan de hand van de data van gebruikers stuur je hen bijvoorbeeld gerichte reclame, je strijkt een commissie op per transactie op je platform of je laat gebruikers lidgeld betalen. Op basis van dergelijke verdienmodellen kun je investeerders proberen te overtuigen zodat je over voldoende middelen beschikt om je applicatie ook daadwerkelijk te bouwen en te lanceren.
Indien een bedrijf echter een gedistribueerde toepassing lanceert, die gebruikmaakt van een technologie zoals blockchain, vallen deze inkomstenbronnen grotendeels weg. De applicatie is immers niet langer onder de exclusieve controle van het bedrijf, maar wordt collectief beheerd door verschillende participanten op het blockchainnetwerk. Hoe kan een bedrijf in zo'n situatie met een overtuigend businessmodel investeerders aantrekken en er zelf ook nog een centje aan verdienen? Het antwoord is de ICO, wat staat voor *Initial Coin Offering*. Bij een ICO worden nieuwe virtuele tokens (jetons, *supra* 2.6. Tokens) uitgegeven. Die tokens kunnen nieuwe virtuele munten zijn, maar het kan ook onder meer gaan om jetons die nodig zijn om gebruik te maken van een specifieke gedistribueerde toepassing. In eerste instantie publiceert het bedrijf een *whitepaper* om de investeerders te overtuigen. Daarna volgt de ICO-periode, waarin de investeerders, meestal voor een vast bedrag, virtuele tokens kunnen kopen. Daarna wordt de applicatie gebouwd en gelanceerd. Indien de applicatie een succes wordt, zal de vraag naar en dus ook de waarde van de tokens toenemen. Het aantal gecreëerde virtuele tokens is immers beperkt, hoewel ze doorgaans wel kunnen worden opgedeeld. De investeerders kunnen na de ICO-periode naar eigen goeddunken beslissen wanneer ze tokens aan- of verkopen.
Een voorbeeld van een dergelijke applicatie is *FirstBlood*, een gedecentraliseerd platform voor competitie in onlinegames. Spelers kunnen elkaar uitdagen en de winnaar krijgt een beloning. Een tweede voorbeeld is *Storj*, wat een gedistribueerde cloudopslag moet worden. Een participant betaalt als hij opslag op andere computers wil gebruiken en wordt betaald als hij schijfruimte aanbiedt.
Gestuwd door de golven van de Bitcoin- en blockchainhype kon zo snel geld opgehaald worden. De eerste ICO was die voor *Ethereum*, het eerste en meest populaire blockchaingebaseerde smartcontractplatform. Tijdens de ICO-periode in 2014 kochten investeerders ether – de virtuele munt van Ethereum – voor een prijs van 1 bitcoin voor 2.000 ethers, wat toen overeenkwam met 35 tot 40 dollarcent. De waarde van de ether piekte in januari 2018 tot meer dan 1.400 dollar, om terug te zakken tot, op het moment van schrijven, ongeveer 140 dollar, wat nog steeds een tot de verbeelding sprekende *return-on-investment* is. *FirstBlood* haalde in 2016 op enkele minuten tijd 5,5 miljoen dollar op en *Tezos* haalde in 2017 232 miljoen dollar op voor een nieuw smart-

contractnetwerk, gebaseerd op blockchain. *EOS*, een nieuw smartcontractplatform, haalde in 2018 het recordbedrag van meer dan vier miljard dollar op. De tien projecten met de kortste duur (uitgedrukt in seconden) verzamelden fondsen aan een gemiddelde snelheid van 300.000 dollar per seconde. In 2017 werd via ICO's 6,2 miljard dollar opgehaald, in 2018 was dit al ruim 21 miljard dollar, om in 2019 terug te vallen op minder dan anderhalf miljard[211]. Volgens Custer bloedt het ICO-model dood door het verdwijnen van de hype en toename van de regulering[212].

Bij een ICO wordt dus een deel van de tokens op voorhand toegekend. Dit is verschillend van Bitcoin, waar de virtuele munten ontgonnen werden of nog ontgonnen moeten worden. De toegekende hoeveelheden virtuele tokens in ICO's zijn slechts getallen die in de blockchain of het smart contract – computercode op de blockchain – geregistreerd worden: bijvoorbeeld 1.000 virtuele tokens worden toegekend aan pseudoniem A, 2.000 aan pseudoniem B en 10.000 aan pseudoniem C. In het geval van *Gnosis* hielden de oprichters 95% van de tokens voor zichzelf en werd maar 5% via een ICO te koop aangeboden[213]. Dit zijn allemaal 'voorgedolven' (*pre-mined*) virtuele munten, wat niet uitsluit dat achteraf nog nieuwe virtuele tokens gecreëerd worden, bijvoorbeeld via *mining*.

De meeste ICO's worden op een bestaand blockchainplatform, momenteel meestal Ethereum, uitgegeven. In dat geval wordt er op het blockchainplatform een nieuw smart contract gepubliceerd dat onder meer bijhoudt welk pseudoniem hoeveel tokens bezit. Dit is het geval voor onder meer *FirstBlood* en *Storj*. Een eenvoudig smart contract kan al volstaan[214]. Een andere manier is dat er een volledige nieuwe blockchain, en dus ook blockchainnetwerk, gelanceerd wordt. Dat laatste is gebeurd voor onder meer Ethereum, Tezos en EOS.

### 3.14.2. ***Risico's***

Bij ICO's moeten evenwel een aantal niet te verwaarlozen risico's aangestipt worden. Volgens een schatting uit december 2017 komt ruim 10% van de investeringen voor ICO's terecht bij hackers[215]. De blockchain is dan misschien wel veilig, maar de zaken eromheen zijn dat niet altijd. Zo kan een hacker een phishingmail versturen naar investeerders, waarin hij zich voordoet als een gerenommeerd bedrijf dat een ICO aanbiedt. Een andere aanval gaat als volgt. Een investeerder stuurt doorgaans een bedrag in een bestaande virtuele munt naar een pseudoniem (adres of rekening), en krijgt de tokens in de plaats. Een hacker kan echter op de website van het organiserende bedrijf

211 Zie www.coinschedule.com.

212 C. Custer, *The ICO May Be Truly Dead*, Longhash, 30 september 2019, https://en.longhash.com/news/the-ico-is-well-and-truly-dead.

213 A. Hertig, 'ICO Insanity? $300 Million Gnosis Valuation Sparks Market Reaction', *Coindesk*, 26 aril 2017, www.coindesk.com/ethereum-ico-irrationality-300-million-gnosis-valuation-sparks-market-concerns.

214 M. Neto, 'How to do an ICO on Ethereum in less than 20 minutes', *Medium*, 20 maart 2018, https://medium.com/bitfwd/how-to-do-an-ico-on-ethereum-in-less-than-20-minutes-a0062219374.

215 EY, 'EY Research: Initial Coin Offerings (ICOs)', december 2017, www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/%24File/ey-research-initial-coin-offerings-icos.pdf.

inbreken en dit pseudoniem vervangen door het zijne. Dit resulteerde in de zomer van 2017 bijvoorbeeld tot een verlies van 7,4 miljoen dollar bij een bepaalde ICO[216].
Vanuit Vietnam werden ook twee ICO's gelanceerd, *Pincoin* en *iFan*. Ze wisten 32.000 investeerders te overtuigen, voor een totaal bedrag van 660 miljoen dollar. In april 2018 bleek dat het om bedrog ging. De fraudeurs verdwenen met de noorderzon[217].
Doordat vaak nog een specifieke juridische kader ontbreekt, genieten de gedupeerden in vele landen nog onvoldoende bescherming. Een bekend voorbeeld van een fraudeleuze ICO's is *BitConnect*, wat op een gegeven moment met een waarde van 2,6 miljard dollar tot de twintig grootste virtuele munten behoorde. Het was echter ponzifraude (*i.e.* beleggingen worden aangeboden met de belofte van een goed rendement, waarbij het geld van de beleggers niet wordt geïnvesteerd maar ten goede komt aan oplichters[218]) en crashte begin 2018[219]. *OneCoin* is nog een geval van ponzifraude, ter waarde van 2,3 miljard dollar[220].
Het is niet steeds zo dat een blockchain nodig is om geld op te halen. Naarmate ICO's meer gereguleerd worden, zullen deze waarschijnlijk minder voorkomen, aangezien het gebruik van een ICO geregeld werd gezien als een makkelijke manier om ongereguleerd investeerders aan te trekken.
De ICO-*whitepapers* zijn trouwens niet-gereguleerde documenten die geen audit hebben ondergaan. Daardoor is er geen zekerheid over de nauwkeurigheid of de correctheid van de erin vermelde claims. Essentiële technische en juridische kwesties ontbreken mogelijks of het uiteindelijke smart contract kan afwijken van wat in de ICO beschreven is. Het is ook steeds de vraag of de beloftes realistisch zijn en of de beloofde toepassing er wel ooit zal komen. De ICO's worden vaak gelanceerd door start-ups, wat sowieso al een risico met zich meebrengt.
Op het moment van de ICO is er meestal enkel het idee of in het beste geval een prototype. Dit zou dan gelanceerd worden op een bestaand blockchainnetwerk, meestal Ethereum, met alle beperkingen die dit platform kent. Gegeven de beperkte capaciteit van Ethereum, kan bijvoorbeeld één succesvol smart contract het hele netwerk vertragen en daarmee ook alle smart contracts op het Ethereum-platform, alsook alle gedistribueerde applicaties die van die smart contracts gebruikmaken. In december 2017 was één gedistribueerde applicatie, *CryptoKitties,* zo populair dat het hele Ethereum-netwerk verzadigde.

---

216 L. Franceschi-Bicchierai & J. Pearson, 'Hacker Allegedly Steals $7.4 Million in Ethereum with Incredibly Simple Trick', *Motherboard*, 17 juli 2017, https://motherboard.vice.com/en_us/article/zmvg58/hacker-allegedly-steals-dollar74-million-in-ethereum-with-incredibly-simple-trick.
217 W. Suberg, 'Vietnam: Pincoin, Ifan ICOs Exposed As Scams That Allegedly Stole $660 Million', *CoinTelegraph*, 10 april 2018, https://cointelegraph.com/news/vietnam-pincoin-ifan-icos-exposed-as-scams-that-allegedly-stole-660-million.
218 Zie www.fsma.be/nl/ponzifraude.
219 Zie 'How BitConnect pulled the biggest exit scheme in cryptocurrency', *The Next Web*, 17 januari 2018, https://thenextweb.com/hardfork/2018/01/17/bitconnect-bitcoin-scam-cryptocurrency.
220 M.J. Zuckerman, 'Chinese Prosecutors Charge Final Suspects In $2.3 Bln OneCoin Investigation', *CoinTelegraph*, 23 mei 2018, https://cointelegraph.com/news/chinese-prosecutors-charge-final-suspects-in-23-bln-onecoin-investigation.

Het aankopen van tokens doe je trouwens doorgaans in een bestaande virtuele munt, bijzonder volatiel virtueel geld dus. Stel dat tijdens of vlak na een ICO de waarde van de virtuele munt sterk zou dalen, dan is er misschien alsnog onvoldoende kapitaal om het project te financieren.

### 3.14.3. *Regulering*

De eerste ICO's waren geheel ongereguleerd en werden dus vaak vooral gezien als een gemakkelijke manier om ongereguleerd investeringen aan te trekken. Het juridisch vacuüm waarin ICO's zich bevonden, wordt ondertussen stapsgewijs door overheden wereldwijd gedicht[221]. In onder andere de Verenigde Staten, Canada, Singapore, Australië en Japan is er al regelgeving. In Europa is de discussie volop bezig. China bijvoorbeeld heeft een volledig verbod ingevoerd[222].

De term *token* is vrij vaag en kan in beginsel van alles zijn: jetons die nodig zijn om gebruik te maken van een gedistribueerde toepassing, virtueel geld, een representatie van grondstoffen of zelfs aandelen.

Afhankelijk van het karakter van de tokens kan dus andere wetgeving van toepassing zijn[223]. De Amerikaanse toezichthouder SEC (U.S. Securities and Exchange Commission) heeft bijvoorbeeld al aangegeven dat indien een token voldoet aan de definitie van een effect, het handelsplatform geregistreerd moet zijn bij de SEC (ofwel vrijgesteld van registratie)[224]. Er is dus een benadering van elk individueel geval nodig om te achterhalen onder welke definities en regelgeving de token valt.

De SEC houdt het niet bij woorden. Zo beschuldigde zij in december 2019 het bedrijf *Shopin* en zijn oprichter van verkoop van ongeregistreerde effecten. Bij een ICO haalden *Shopin* 42 miljoen dollar op. Het beloofde platform werd echter nooit gebouwd en de investeringen werden ten onrechte gebruikt voor persoonlijke doeleinden[225]. Recenter heeft de SEC een gerechtelijk bevel ingediend om Telegram te dwingen uit te leggen hoe de 1,7 miljard dollar die bij een ICO zijn opgehaald besteed werden[226]. Ook hier gaat het volgens de SEC om de verkoop van ongeregistreerde effecten. Dit zijn maar twee voorbeelden om aan te geven dat ICO's de SEC werk bezorgen en dat ook ICO's

221 Zie L. Overwater & B. Custers, 'De regulering van Initial Coin Offerings en cryptocurrencies. Een vergelijking van verschillende landen', *Computerrecht* 2018/208; A. De Backer en V. De Boe, 'Smart contracts in de financiële sector: grote verwachtingen en regulatoire uitdagingen', *Computerrecht* 2017/252; H. Schuringa, 'Enkele civielrechtelijke aspecten van blockchain', *Computerrecht* 2017/254.

222 Voor een overzicht van de regulering per land, zie www.bitcoinmarketjournal.com/ico-regulations.

223 Simont Braun, *ICO'S in Belgium and Europe: a legal perspective*, februari 2018, www.simontbraun.eu/fr/news/news-corporate-banking-and-finance/2126-icos-in-belgium-and-europe-a-legal-perspective.

224 SEC, *Statement on Potentially Unlawful Online Platforms for Trading Digital Assets*, 7 maart 2018, www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading. Zie ook SEC, *Investor Bulletin: Initial Coin Offerings*, 25 juli 2017, www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings.

225 *Press release: SEC Charges Founder, Digital-Asset Issuer With Fraudulent ICO*, U.S. Securities and Exchange Commission, 11 december 2019, https://www.sec.gov/news/press-release/2019-259.

226 C. Osborne, 'SEC seeks to force Telegram to reveal how $1.7bn ICO funds were spent', *ZDNet*, 3 januari 2020, https://www.zdnet.com/article/sec-seeks-to-force-telegram-to-reveal-how-1-7bn-in-ico-funds-were-spent/.

niet ontsnappen aan het bestaand regulerend kader. De SEC lanceerde ter bewustmaking zelfs een eigen, valse ICO, genaamd *HoweyCoins*[227].

Bij gebrek aan specifieke regulering is het van belang om bij een ICO stil te staan bij de mogelijke toepasselijkheid van verschillende bestaande regelgeving[228]. Een aantal Europese richtlijnen en verordeningen kunnen immers mogelijk van toepassing zijn, bijvoorbeeld de Prospectusverordening (publiek aanbieden en verhandelen van effecten)[229], de *Markets in Financial Instruments Directive* en *Regulation* (MiFID II en MIFIR)[230], de *Alternative Investment Fund Managers Directive* (AIFMD)[231], de *Market Abuse Regulation* (MAR)[232] en de *Fifth Anti-Money Laundering Directive* (AMLD5)[233]. Met betrekking tot Nederlandse wetgeving en toezicht dient te worden gekeken naar de mogelijke toepasselijkheid van de Wet op het financieel toezicht (Wft), maar denk bijvoorbeeld ook aan de specifieke regels voor verkoop aan consumenten en consumentenzaken.

De vraag kan worden gesteld in hoeverre een *whitepaper* overeenkomt met een prospectus bij een beursgang[234]. Wanneer we kijken naar een *whitepaper* zoals die van The DAO, lijkt dit in elk geval niet te voldoen aan de vereisten van een prospectus. Volgens artikel 3, lid 1 Prospectusrichtlijn is er een prospectusplicht wanneer effecten aan het publiek worden aangeboden. Artikel 2, lid 1, sub a Prospectusrichtlijn bepaalt dat ef-

227 *ICO – HoweyCoins*, U.S. Securities and Exchange Commission. https://www.investor.gov/howeycoins.

228 Statement ESMA, 'ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements', www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf.

229 Richtlijn 2003/71/EG van het Europees Parlement en de Raad van 4 november 2003 betreffende het prospectus dat gepubliceerd moet worden wanneer effecten aan het publiek worden aangeboden of tot de handel worden toegelaten en tot wijziging van Richtlijn 2001/34/EG, *Pb.L.* 31 december 2003, afl. 345, 64. Verordening 2017/1129 van het Europees Parlement en de Raad van 14 juni 2017 betreffende het prospectus dat moet worden gepubliceerd wanneer effecten aan het publiek worden aangeboden of tot de handel op een gereglementeerde markt worden toegelaten en tot intrekking van Richtlijn 2003/71/EG, *Pb.L.* 30 juni 2017, afl. 168, 12.

230 Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU, *Pb.L.* 12 juni 2014, afl. 173, 349; Verordening nr. 600/2014 van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten in financiële instrumenten en tot wijziging van Verordening nr. 648/2012, *Pb.L.* 12 juni 2014, afl. 173, 84.

231 Richtlijn 2011/61/EU van het Europees Parlement en de Raad van 8 juni 2011 inzake beheerders van alternatieve beleggingsinstellingen en tot wijziging van de Richtlijnen 2003/41/EG en 2009/65/EG en van de Verordeningen nr. 1060/2009 en (EU) nr. 1095/2010, *Pb.L.* 1 juli 2011, afl. 174, 1.

232 Verordening nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (Verordening marktmisbruik) en houdende intrekking van Richtlijn 2003/6/EG van het Europees Parlement en de Raad en Richtlijnen 2003/124, 2003/125/EG en 2004/72/EG van de Commissie, *Pb.L.* 12 juni 2014, afl. 173, 1.

233 Richtlijn 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU, *Pb.L.* 19 juni 2018, afl. 156, 43.

234 Voor een database van whitepapers, zie https://whitepaperdatabase.com.

fecten voor toepassing van de richtlijn verhandelbare effecten moeten zijn in de zin van artikel 1, punt 4 Richtlijn 93/22/EEG[235]. Volgens die richtlijn zijn dat:

– *aandelen en andere met aandelen gelijk te stellen waardepapieren;*
– *obligaties en andere schuldinstrumenten die op de kapitaalmarkt verhandelbaar zijn;*
– *alle andere gewoonlijk verhandelde waardepapieren waarmee die effecten via inschrijving of omruiling kunnen worden verworven of die in contanten worden afgewikkeld;*
– *met uitsluiting van betaalmiddelen.*

## 3.15. Slotopmerkingen

Bitcoin komt voort uit de *cypherpunk*-beweging[236], die door middel van cryptografie sociale en politieke verandering teweeg wil brengen. Vanuit deze anti-establishmentfilosofie kwam Mike Hearn, één van de voornaamste leden van het Bitcoin-core team, in 2016 tot de conclusie dat het Bitcoin-project gefaald is. Hij verliet het Bitcoin-core team en verkocht al zijn bitcoins. Hij formuleerde het als volgt[237]: '*What was meant to be a new, decentralised form of money that lacked 'systemically important institutions' and 'too big to fail' has become something even worse: a system completely controlled by just a handful of people*', vermoedelijk verwijzend naar die enkele grote delvers, maar mogelijks ook naar de handelsplatformen, wallet beheerders en misschien zelf het Bitcoin core team.

Bitcoin blijft niettemin de eerste en nog steeds populairste blockchaintoepassing. Het heeft enkel daardoor al een belangrijke verdienste: de introductie van het technologische concept van de blockchain en het populariseren van het idee van het distribueren van vertrouwen over meerdere participanten. Het is een idee dat al langer onder cryptografen leeft, namelijk dat alles wat met een vertrouwde autoriteit gedaan kan worden, ook zonder die autoriteit mogelijk is. Het gegeven dat iets technisch mogelijk is, betekent natuurlijk niet automatisch dat het ook maatschappelijk wenselijk is. In het geval van Bitcoin komt er bijvoorbeeld bijzonder veel risico te liggen bij de eindgebruiker, die niet langer beschikt over de traditionele vangnetten wanneer het verkeerd loopt. Het lijkt allerminst evident om dergelijke vangnetten te voorzien zonder het gedistribueerde karakter van virtuele munten aan te tasten. Het idee van Bitcoin en de achterliggende blockchaintechnologie was de creatie van een systeem dat toelaat om waarde te transfereren, zonder een rol voor banken noch overheden. Die overheden zitten – gelukkig? – niet stil en de EU is al begonnen om op zijn minst de handelsplatformen en beheerders van onlineportefeuilles door de lidstaten te laten onderwerpen aan regelgeving. Tegen 10 januari 2020 moe(s)ten de lidstaten wetgeving aannemen om han-

235 Richtlijn 93/22/EEG van de Raad van 10 mei 1993 betreffende het verrichten van diensten op het gebied van beleggingen in effecten, *Pb.L.* 11 juni 1993/141, p. 27.

236 E. Hughes, 'A Cypherpunk's Manifesto', *Activism*, 9 maart 1993, www.activism.net/cypherpunk/manifesto.html.

237 J. Kelly, 'Lead developer quits bitcoin saying it 'has failed'', *Reuters*, 15 januari 2016, www.reuters.com/article/us-global-technology-bitcoin/lead-developer-quits-bitcoin-saying-it-has-failed-idUSKCN0UT2II.

delsplatformen en walletaanbieders te registreren. Het idee van een financieel systeem dat geheel ontsnapt aan overheidscontrole wordt daarmee genuanceerd. Toch is er nog werk aan de winkel, niet alleen regelgevend, maar ook wat betreft het bewustzijn bij de burgers, die zich geregeld laten misleiden. Bewustmakingscampagnes zoals het Belgische *Te Mooi Om Waar Te Zijn*[238] zijn dan ook nuttige initiatieven.

Het is bovendien ironisch dat virtuele munten, die zich net beroepen op transparantie, ook bijzonder niet-transparante kanten hebben. Wat zullen morgen de koers en de transactiekosten zijn? Welke entiteiten staan in voor het veilig houden van mijn transactie? Wat gebeurt er eigenlijk in dit hele proces om mijn transactie te verwerken en wie is daarin betrokken? Deze vragen komen gedeeltelijk voort uit het ongereguleerde karakter, maar maken ook onlosmakelijk deel uit van een breder technologisch gegeven. Er is tot op bepaalde hoogte immers sprake van een *black box*. Hoe complexer de technologie wordt die we gebruiken, hoe minder inzicht we hebben in de werking en hoe meer we er dus maar gewoon op moeten vertrouwen dat alles correct blijft werken. Een mogelijke gedeeltelijke oplossing voor dit laatste probleem zou kunnen worden gevonden bij *stable coins* gelanceerd door overheden, zoals in Venezuela en Rusland. Ondanks de bedenkelijke drijfveren van deze landen, is het idee van overheidsgereguleerde *stable coins* het op zich waard om te onderzoeken. Het kan immers zo een platform bieden aan burgers en ondernemingen om snel en goedkoop zowel eenvoudige als complexe waardeuitwisselingen mogelijk te maken, terwijl tegelijkertijd onzekerheden weggenomen worden door het vermijden van hoge koersvolatiliteit en het bieden van juridische garanties.

Daarnaast stellen er zich technisch ook nog grote uitdagingen, onder meer op het vlak van schaalbaarheid. Op dit vlak zijn er al initiatieven genomen voor verschillende virtuele munten. In de zomer van 2017 werd in Bitcoin *SegWit* ingevoerd, wat inhoudt dat een deel van de transactie buiten de blockchain bewaard wordt, waardoor de capaciteit van het netwerk toeneemt. Een ander ambitieus, maar ook omstreden[239] project is het ondertussen actieve *Lightning Network*. Het is een soort laag of netwerk boven op Bitcoin dat bliksemsnelle transacties belooft met een capaciteit van miljarden transacties en lage transactiekosten, maar dat wel vereist dat er eerst virtueel geld geblokkeerd wordt. Ook andere virtuele munten hebben gelijkaardige initiatieven lopen. Ethereum heeft een systeem geïnspireerd op Bitcoins Lightning-netwerk, genaamd Plasma[240], werkt aan *sharding* (een systeem waarbij niet iedereen alles hoeft te valideren)[241] en aan *sidechains*, waarbij meerdere Ethereum blockchains naast en met elkaar werken. De technologie achter de virtuele munt van morgen is overduidelijk in volle evolutie en

238 https://temooiomwaartezijn.be.

239 J. Fyookball, 'Mathematical Proof That the Lightning Network Cannot Be a Decentralized Bitcoin Scaling Solution', *Medium*, 27 juni 2018, https://medium.com/@jonaldfyookball/mathematical-proof-that-the-lightning-network-cannot-be-a-decentralized-bitcoin-scaling-solution-1b8147650800.

240 L. Schor, 'Explained: Ethereum Plasma', *Medium*, 28 mei 2018, https://medium.com/@argongroup/ethereum-plasma-explained-608720d3c60e.

241 R. Jordan, 'How to Scale Ethereum: Sharding Explained', *Medium*, 10 januari 2018, https://medium.com/prysmatic-labs/how-to-scale-ethereum-sharding-explained-ba2e283b7fce.

één van de grote uitdagingen blijft schaalbaarheid, namelijk het verhogen van de capaciteit.

Ten slotte dient opgemerkt te worden dat er meestal sprake is van blockchain, maar dat er meer is dan blockchain. Zo is er IOTA[242], een virtuele munt die vertrekt vanuit een ander concept, genaamd *The Tangle*. Daarbij zijn er geen blokken, delvers of transactiekosten. Om een transactie te doen, moet je ook twee andere transacties valideren. Blockchain en *The Tangle* behoren beide tot de bredere categorie van *Distributed Ledger Technology* (DLT), waarbij verschillende participanten in een netwerk collectief garanderen dat de regels nageleefd worden en collectief gegevens bewaren en veilig houden. Het is dus niet ondenkbaar dat virtuele valuta binnen een aantal jaar volledig afgestapt zijn van het oorspronkelijke blockchainconcept, maar andere DLT-concepten zullen toepassen.

De toekomst van virtuele valuta is moeilijk te voorspellen. Hoogstwaarschijnlijk zullen ze blijven bestaan en zal hun belang toenemen. De technologie zal echter nog sterk evolueren om zo veel als mogelijk een antwoord te bieden op de uitdagingen die zich stellen. Ook het juridisch kader zal zich de komende jaren verder ontwikkelen, voornamelijk ter bescherming van de consument en ter voorkoming van fraude. Vandaag de dag zijn er meer dan 2.000 virtuele munten, wat bijzonder onoverzichtelijk is. Niet al deze virtuele valuta zullen blijven bestaan. De virtuele valuta die morgen de norm zijn, bestaan misschien thans nog niet en omgekeerd. Het is dus goed om zich er bewust van te zijn dat er veel onzekerheid is en dat er talrijke risico's zijn. De overheid zal dus onvermijdelijk verder haar verantwoordelijkheid moeten nemen.

242 www.iota.org.

# 4. Blockchain en vastgoed

Sinds blockchaintechnologie bij het grote publiek bekend is geworden, zijn er tal van voorstellen gedaan om blockchain in te zetten in de vastgoedpraktijk waaronder de overdracht en registratie van onroerende zaken.[243] Naast veel juridisch onderzoek naar de mogelijkheden en problemen[244] zijn er daadwerkelijk enkele proefprojecten uitgevoerd. In dit hoofdstuk wordt de stand van zaken besproken. 4.1. legt uit hoe het Nederlandse systeem werkt, en wat de rol van notaris en Kadaster hierbij is. Dit zal worden uitgelegd zonder veel juridische voorkennis te veronderstellen. Daarna analyseert 4.2. op welke punten blockchaintechnologie zou kunnen worden ingezet. Vervolgens bespreken 4.3., 4.4. en 4.5. drie manieren waarop blockchain als een vervanging gebruikt zou kunnen worden in de huidige vastgoedketen. Hierbij worden ook enkele buitenlandse experimenten besproken. De nadruk ligt hierbij op rechtshandelingen rond de registratie van onroerend goed. Daarnaast zijn er nog tal van andere kwesties in de vastgoedpraktijk, zoals huur en financiering. Deze zullen hier niet uitgebreid behandeld worden, maar 4.6. stipt deze kort aan.

## 4.1. Vastgoed in Nederland: register, Kadaster en notaris

Het probleem bij eigendom van vastgoed is dat eigendom niet zo goed kan worden afgeleid uit fysieke kenmerken, met name als het gaat om een claim op een niet afgesloten perceel. Of iemand eigenaar is, moet dan ook op een andere manier worden vastgesteld. In veel landen wordt de eigendom vastgesteld door te bewijzen dat de eigendom is verkregen van de vorige rechtmatige eigenaar. Dit gebeurt meestal met een geldige leveringsakte (in het Engels '*deed*') waarmee op juridisch geldige wijze de eigendom is overgegaan. Om vast te stellen dat de vorige eigenaar rechtsgeldig eigenaar was, moet natuurlijk weer worden bewezen dat die vorige eigenaar de eigendom van de eigenaar daarvoor heeft verkregen enzovoort. In landen zoals Engeland die geen register hebben, is het vaststellen van eigenaarschap daarom kostbaar en tijdrovend.

243 De term 'vastgoed' wordt hier gebruikt als synoniem voor de juridisch correctere term 'onroerend goed' of beter nog 'onroerende zaak' (art. 3:3 BW).

244 Zie ook M. Schellekens, T.F.E. Tjong Tjin Tai, W. Kaufmann, F. Schemkes & R. Leenes, 'Blockchain en het recht', WODC rapport 2019, waarin een use case wordt behandeld over het scheepsregister (wat vergelijkbare problemen oplevert als het register van onroerend goed).

In veel landen is er daarom een *register* voor land en andere onroerende zaken. In Nederland is dit verplicht op grond van artikel 3:10 BW.[245] Het register is bedoeld om leveringsaktes en andere stukken op te slaan die betrekking hebben op de onroerende zaak. Het register is niet meer dan een opslag, een grote 'dossierkast', ook als het geautomatiseerd is. Het nadeel van zo'n eenvoudig register is dat er bij verkoop van een woning nog steeds moet worden gecontroleerd of de keten van aktes klopt. Het is dan ook logisch om een stap verder te gaan. Er wordt dan ook bijgehouden of de leveringsakte het bedoelde effect had, of die akte inderdaad klopte, en er wordt bijgehouden wie uiteindelijk volgens de geregistreerde gegevens de eigenaar is. Zo'n registratie gaat verder dan een gewoon register. In Nederland heet dit de *kadastrale registratie*.[246] Deze wordt bijgehouden door de Dienst voor het Kadaster en de openbare registers,[247] die we meestal gewoon Kadaster noemen. Overigens wordt de kadastrale registratie ook wel 'het kadaster' genoemd, maar omdat dit verwarrend is zullen we dat hier niet doen. Het Kadaster houdt dus het register van onroerend goed bij én de kadastrale registratie. De rol van het Kadaster is hierbij actief: de 'bewaarder' weigert stukken die niet voldoen aan de wettelijke eisen (art. 3:19 en 3:20 BW).[248] Daardoor is de inhoudelijke kwaliteit van het register gewaarborgd.

De registratie in de kadastrale registratie geeft niet altijd correct aan wie eigenaar is. Het is bijvoorbeeld mogelijk dat achteraf blijkt dat een akte is gesloten onder dwang of een ontbindende voorwaarde is vervuld. Ook andere feiten, zoals het overlijden van de eigenaar (waarna de erfgenamen eigenaar zijn geworden), worden niet vanzelf in de kadastrale registratie opgenomen. Daarom wordt het Nederlandse stelsel een negatief stelsel genoemd. Als de leveringsakte niet wordt ingeschreven, kan de nieuwe eigenaar geen eigenaar worden. Omgekeerd betekent de inschrijving echter ook niet dat vaststaat dat de geregistreerde eigenaar daadwerkelijk eigenaar is.[249] De kadastrale registratie geeft een grote mate van zekerheid maar geen absolute zekerheid. Meestal zal een partij die hier belang bij heeft ervoor zorgen dat het register en de kadastrale registratie worden aangepast.[250]

Naast de registratie van eigendom is het register van onroerend goed en het Kadaster ook nuttig voor registratie van andere rechten op vastgoed of andere relevante gegevens.[251] Een voorbeeld is het recht van hypotheek. De bank die een hypothecaire lening

245 'Registergoederen zijn goederen voor welker overdracht of vestiging inschrijving in daartoe bestemde openbare registers noodzakelijk is.' Art. 3:16 lid 1 BW bepaalt: 'Er worden openbare registers gehouden, waarin feiten die voor de rechtstoestand van registergoederen van belang zijn, worden ingeschreven.' In de Kadasterwet worden verdere details geregeld.

246 Zie hierover J.A. Zevenbergen & J. de Jong, 'Inleiding', in: J. de Jong e.a., *Naar een meer positief stelsel van grondboekhouding?*, preadvies Vereniging voor Burgerlijk Recht, Kluwer 2003.

247 Art. 1 lid 1 Kadasterwet en art. 2 Organisatiewet Kadaster.

248 Zie o.a. de eisen in art. 18-47 Kadasterwet. Een voorbeeld is de inschrijving van erfopvolging: hiervoor is een notariële (of Europese) verklaring van erfrecht nodig (art. 27 en 28 Kadasterwet).

249 In Duitsland is er wel een grotendeels positief stelsel. Zie uitvoerig over de verschillende stelsels B. Verheye, 'Real estate publicity in a blockchain world: a critical assessment', *European Property Law Journal* 2017 6(3), pp. 441-476.

250 Zie art. 3:27-29 BW.

251 Op grond van art. 3:17 BW kunnen bepaalde gegevens al worden opgenomen in het register. Daarnaast kan de kadastrale registratie nog meer feiten bevatten.

verstrekt, krijgt een hypotheekrecht, wat inhoudt dat zij het vastgoed mag verkopen als de lening niet wordt afgelost. Andere voorbeelden zijn een beslag dat is gelegd op het vastgoed en erfdienstbaarheden zoals een recht van opstal.
Er zijn verschillende manieren waarop de toegang tot het register en de kadastrale registratie kunnen worden geregeld. Een mogelijkheid is dat partijen zelf aktes in het register kunnen laten inschrijven. Dan zou iedereen zelf een akte[252] kunnen opstellen en deze laten inschrijven. De Nederlandse wetgever heeft echter een ander systeem gekozen.[253] Levering van onroerend goed kan alleen plaatsvinden met een notariële akte (art. 3:89 BW), dat wil zeggen een akte die door een notaris is opgesteld. De reden voor deze keuze, die in 1956 is gemaakt, is dat voorheen te vaak fouten werden gemaakt in de aktes die werden ingeschreven, waardoor onduidelijk was wat de juridische toestand van onroerend goed was.[254] De inschakeling van de notaris is dus bedoeld om de kwaliteit van het stelsel te verhogen. De notaris is verplicht om te zorgen dat de akte het bedoelde resultaat realiseert. Hij is dat niet alleen verplicht omdat hij daarvoor betaald wordt door zijn opdrachtgever, maar ook is hij dat verplicht tegenover derden die hier belang bij hebben. Als hij een fout maakt in de akte, is hij hiervoor aansprakelijk.
Daarnaast is de notaris ook verplicht om te zorgen voor allerlei andere dingen.[255] Hij moet bijvoorbeeld controleren op de identiteit en wilsbekwaamheid van partijen, nagaan of partijen echt begrijpen wat er gaat gebeuren, en controles uitvoeren op verdachte transacties (in het bijzonder witwassen). Verder gaat hij na of het onroerend goed daadwerkelijk geleverd kan worden, zoals of er geen beslag op rust, de eigenaar niet failliet is en er niet nog hypotheekrechten of andere beperkingen op rusten. Tot slot heeft de notaris vaak een rol in de afwikkeling van betalingsverkeer rond de transactie.[256]

## 4.2. Toepassingen van blockchain bij vastgoedtransacties

Als we het Nederlandse stelsel bezien, lijken er verschillende mogelijkheden te bestaan om blockchain in te zetten. In de media, op internet, en in buitenlandse artikelen wordt geregeld ingegaan op de mogelijkheid dat blockchain de hele registratie zou overne-

252 Dit wordt een 'onderhandse akte' genoemd. Dat wil zeggen een akte, namelijk een document bedoeld als bewijs van de bedoeling van partijen (art. 156 lid 1 Rv), die niet door een notaris is opgesteld.
253 Zie hierover T.F.E. Tjong Tjin Tai, 'De blockchain als alternatief voor de notariële praktijk', in: F.W.J.M. Schols & B.C.M. Waaijer (red.), *Financiële zorgplicht van de notaris*, preadviezen KNB 2018, Den Haag: Sdu 2018, p. 99-135.
254 Asser/Bartels en Van Mierlo, *Algemeen goederenrecht*, 3-IV 2013/294.
255 T.F.E. Tjong Tjin Tai, 'De blockchain als alternatief voor de notariële praktijk', in: F.W.J.M. Schols, B.C.M & Waaijer (red.), *Financiële zorgplicht van de notaris*, preadviezen KNB 2018, Den Haag: Sdu 2018, p. 99-135; J.C.H. Melis & B.C.M. Waaijer, *De Notariswet*, 9e dr., Deventer: Wolters Kluwer 2019; H.W. Heyman, S.E. Bartels & V. Tweehuysen, *Vastgoedtransacties. Overdracht*, Den Haag: Boom juridisch 2019.
256 F.W.J.M. Schols &B.C.M. Waaijer (red.), *Financiële zorgplicht van de notaris*, preadviezen KNB 2018, Den Haag: Sdu 2018.

men. Zoals uit de vorige paragraaf bleek, is dat een te simplistische voorstelling van zaken, omdat we verschillende dingen uit elkaar moeten houden.[257]

a) Blockchain kan worden gebruikt als *register*.
b) Blockchain zou ook kunnen dienen om (delen van) de *kadastrale registratie* over te nemen.
c) Blockchain kan ook worden gebruikt als alternatief voor de *verplichte rol* van het Kadaster en/of de notaris. Het zou dan gaan om de rol bij controle van inschrijvingen in het register of de registratie, de rol bij de levering, en de bijstand bij financiele transacties.

Deze drie mogelijkheden worden in de volgende drie paragrafen behandeld. De rol van het Kadaster komt aan de orde in 4.3 en 4.4. 4.5. behandelt de rol van de notaris.
De toepassing van blockchain bij vastgoedregistratie verschilt van toepassingen als Bitcoin, die los staan van de overheid en zelfs tot doel hebben om te opereren zonder overheidsmacht. Eigendomsaanspraken op vastgoed hebben alleen maatschappelijk effect als de overheid deze erkent en bereid is deze te handhaven, anders zal iedereen de aanspraak in de fysieke werkelijkheid kunnen negeren. Een blockchainregister heeft momenteel wettelijke erkenning nodig om effectief te zijn. Een register zal hoogstwaarschijnlijk altijd juridisch ingebed zijn. Het is afhankelijk van het rechtsstelsel en dient daardoor rekening te houden met het optreden van de wetgever, het bestuur en rechterlijke macht. Indien het vertrouwen in deze rechtsstatelijke instituties laag is, zal blockchain hier hoogstwaarschijnlijk geen fundamentele verandering in brengen.

## 4.3. Blockchain als onroerendgoedregister

Een blockchainapplicatie gebruiken als register is mogelijk. De blockchain heeft dan vooral een bewijsfunctie voor rechtshandelingen met registergoederen. De blockchain slaat dan eenvoudigweg alle transacties op, namelijk de aktes of in elk geval een verwijzing daarnaar. In feite is dat dus gewoon de automatisering van het register. Dit is de meest voor de hand liggende toepassing van blockchain binnen deze sector, vooral in landen waar nog geen register bestaat of het register gebrekkig is georganiseerd. In Nederland is er al een register, dat ook al geautomatiseerd is, waardoor de toegevoegde waarde van blockchain hiervoor niet onmiddellijk duidelijk is.
In andere landen zijn er verschillende projecten op dit vlak aangekondigd, waarbij het niet altijd duidelijk is of die projecten alleen zien op een register of ook op kadastrale registratie. Zo is in Zweden, waar al een register bestaat (de *Lantmäteriet*), een pilot project uitgevoerd, dat echter niet landelijk is ingevoerd.[258] Een project in Georgië is

257 Benito Arruñada, 'Blockchain's struggle to deliver impersonal exchange', *Economic Working Paper Series Working Paper No. 1549*, https://econ-papers.upf.edu/papers/1549.pdf.
258 https://blockchan.ge/blockchange-land-registry.pdf.

evenmin wettelijk erkend en heeft slechts een archieffunctie.[259] Een project in Honduras is gestaakt na wisseling in de politieke macht en een project in Ghana schijnt nooit te zijn gematerialiseerd.[260] Het valt op dat de introductie van blockchain tot nu toe tot een proefproject lijkt te komen in landen die al een betrouwbaar register hebben (bijvoorbeeld Zweden en Georgië) en waar de voorgespiegelde voordelen vooral liggen op het gebied van efficiëntie en kostenbesparing,[261] terwijl projecten niet van de grond lijken te komen in landen waar blockchain juist een duidelijk voordeel zou kunnen hebben omdat er nog geen goed register is. Verder wordt de introductie van blockchain regelmatig verdedigd door te wijzen op de behoefte aan digitalisering van het register. In Nederland weten we echter dat het goed mogelijk is te digitaliseren zonder gebruik te maken van blockchain.

Een gevolg van een blockchainregister zou kunnen zijn dat er geen Kadaster meer nodig is om het register te beheren. Dat zou inderdaad tot kostenbesparing kunnen leiden. Op dit moment is dit niet mogelijk, omdat de wet er van uitgaat dat er een bewaarder is die verantwoordelijk is voor de inhoud van het register en die formele eisen controleert (art. 3:18 lid 2 BW). Een blockchainimplementatie zou deze eisen automatisch kunnen laten controleren als onderdeel van het protocol. Overigens is niet duidelijk dat dit zo gemakkelijk zal zijn. De kadasterwet noemt immers veel verschillende soorten feiten die kunnen worden ingeschreven en die niet allemaal afhangen van de 'eigenaar' van het goed.[262] Het probleem is daarenboven dat dit protocol zelf tot op bepaalde hoogte beheerd moet worden als we zeker willen weten dat het overeenkomt met de eisen die de wet stelt. Hierdoor lijkt het niet mogelijk te zijn om met een *permissionless* blockchain te werken. Er zou een *permissioned* blockchain nodig zijn. Het Kadaster zou dan de rol van protocolbeheerder kunnen vervullen.[263] De winst van zo'n oplossing zou dus evenwel beperkt zijn, aangezien er nog steeds een kadastrale organisatie nodig is.

Veel hangt af van de wijze waarop zo'n *permissioned* blockchain is opgezet. Als dit een gesloten *permissioned* blockchain is, verschilt dit nauwelijks van het huidige geautomatiseerde register, waarbij alleen bevoegde partijen stukken kunnen aanbieden aan het register. Men zou dan hoogstens meer partijen kunnen toelaten dan alleen notarissen (*infra* 4.5.). Een openbare *permissioned* blockchain zou wel tot een gewijzigde situatie leiden, maar het register zou op zich ook nu via internet openbaar kunnen worden gemaakt zonder dat er een blockchain aan verbonden is. Ook hier is de reële toegevoegde waarde dus niet onmiddellijk duidelijk.

---

259 N. Lazuashvili, A. Norta & D. Draheim, 'Integration of Blockchain Technology into a Land Registration System for Immutable Traceability: A Casestudy of Georgia', in: C. Di Ciccio e.a. (red.), *Business Process Management: Blockchain and Central and Eastern Europe Forum*, Cham: Springer 2019.

260 http://www.oecd.org/corruption/integrity-forum/academic-papers/Georg%20Eder-%20Blockchain%20-%20Ghana_verified.pdf.

261 Vgl. B. Verheye, 'Real estate publicity in a blockchain world: a critical assessment', *European Property Law Journal* 2017 6(3), pp. 441-476, par. 17.

262 Zie ook 4.4.

263 B. Verheye, 'Real estate publicity in a blockchain world: a critical assessment', *European Property Law Journal* 2017 6(3), p. 441-476, par. 27.

Bovendien zijn er diverse nadelen verbonden aan een blockchainregister. Als het gaat om een *permissioned* blockchain die niet geheel is afgesloten maar voor iedereen via internet te raadplegen is, ontstaat er in beginsel een fundamenteel probleem met privacy.[264]
Daarnaast moet worden gewaarborgd dat de archieffunctie van het register blijft bestaan, ook als er geen interesse meer is om de blockchain in stand te houden.[265]

## 4.4. Blockchain als kadastrale registratie

Een interessantere optie is dat blockchain ook aspecten van de kadastrale registratie op zich gaat nemen. De blockchain is dan meer dan bewijs van rechtshandelingen, aangezien het ook bedoeld is als registratie van de rechtstoestand. Dit kan op verschillende manieren plaatsvinden.

– De blockchain maakt enkele voor de hand liggende afleidingen uit de geregistreerde transacties. Daarmee worden niet noodzakelijk alle mogelijke afleidingen gemaakt. Zoals aangegeven in 4.2. kan een registratie moeilijk volledig zijn omdat er altijd feiten kunnen plaatsvinden die de registratie beïnvloeden maar niet vanzelf of direct geregistreerd worden. Denk bijvoorbeeld aan het overlijden van de eigenaar. Deze beperking neemt niet weg dat het nuttig is een register uit te bouwen tot een registratie waarin enkele afleidingen worden opgenomen. Bij een blockchainregister als besproken in 4.3. lijkt dit ook de bedoeling,[266] zodat dan in feite effectief sprake is van een blockchainregistratie. In elk geval zou de eigendomsoverdracht dan worden afgeleid, namelijk wie volgens de keten van leveringen de huidige eigenaar zou zijn. Ook zouden er dan ten minste een aantal controles moeten plaatsvinden op de transacties, in elk geval met betrekking tot de geldigheid hiervan. Dat betekent opnieuw dat het protocol goed moet zijn vormgegeven om de juiste eisen te stellen aan de transacties. Hieruit volgt dat alleen een *permissioned* blockchain geschikt is, waarbij een officiële instantie moet zorgen dat het protocol de geldigheid van transacties garandeert.
– De blockchain leidt uit de geregistreerde transacties af wat volgens de bekende feiten de juridische toestand is. Dit is hoe het Nederlandse systeem op dit moment werkt. Dit noodzaakt bijvoorbeeld dat er veel meer soorten geregistreerde transacties mogelijk zijn dan alleen eigendomsoverdracht en dus levering van het goed. Ook zouden bijvoorbeeld beslag en hypotheek geregistreerd moeten kunnen worden. Een beslag zou dan bijvoorbeeld in de weg staan aan levering.

---

264 A. Berlee, 'Volledige openbaarheid: het doel voorbij', *WPNR* 2017/7169, A. Berlee, *Access to Personal Data in Public Land Registers*, diss. Maastricht 2018; M. Barbieri & D. Gassen, 'Blockchain – can this new technology really revolutionize the land registry system?', presentatie World Bank, 20-24 maart 2017, download op https://www.notartel.it/export/contenuti_notartel/pdf/Land_Poverty_Conference_Blockchain.pdf.

265 V. Lemieux, 'Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective', *European Property Law Journal* 2017, 6(3), p. 392-440.

266 Ook het bitcoin-protocol werkt in feite zo dat er geen 'saldo' ergens is opgeslagen maar dat het saldo wordt bepaald door alle legitieme transacties op een account op te tellen en het resultaat te bepalen.

– De blockchain is bepalend voor de juridische toestand. Men spreekt ook wel van 'tokenizering': het token representeert dan bindend de juridische toestand van het vastgoed.[267] Dit zou neerkomen op een zogenaamd positief stelsel, namelijk een stelsel waarbij de transfereerbare representatie van goederen op een blockchain bewijs oplevert met betrekking tot de juridische toestand van de goederen. De tokens kunnen dan door het gebruik van smart contracts ontvangen, geblokkeerd en getransfereerd worden.

De voorstellen om blockchain te gebruiken als register voor vastgoedtransacties lijken zich niet altijd bewust te zijn van deze verschillende nuances. Er moet dus evenwel een belangrijk onderscheid worden gemaakt tussen drie mogelijke functies. Is het register bedoeld als afspiegeling van de rechtstoestand (bewijsfunctie), een vereiste voor de rechtshandeling (leveringsvereiste), of zou het bepalend moeten zijn voor de rechtstoestand (constitutief)? Voor de laatste twee functies is een wettelijke grondslag nodig, die op dit moment ontbreekt. Er is wel een grondslag voor registratie van de levering, namelijk artikel 3:89 BW.
Deze verschillende invullingen van een blockchainregistratie lopen allemaal ook tegen enkele bezwaren aan. De belangrijkste bezwaren hangen samen met de fundamentele aanname van een blockchainimplementatie dat het bezit van de private sleutel als enige bepalend is voor de bevoegdheid om over het onroerend goed te beschikken: zonder private sleutel is levering niet mogelijk en met het bezit van de private sleutel heb je per definitie de juridische bevoegdheid. Die gedachtegang levert evenwel problemen op bij verschillende gevallen waar dit niet in overeenstemming is met de werkelijkheid:[268]

– De private sleutel wordt gehackt.[269]
  Is de levering dan geldig? Dit is allerminst een fictieve gedachte. Regelmatig zijn er berichten over hacks waarbij bitcoins worden gestolen doordat een onbevoegde de beschikking kreeg over de private sleutel.[270] Overigens is het maatschappelijk ook omstreden of iedere eigenaar verplicht kan worden om een private sleutel aan te maken en geheim te houden.
– De private sleutel raakt verloren, bijvoorbeeld door een computercrash zonder dat er een back-up is of doordat het wachtwoord is vergeten. Ook dit gebeurt regelma-

267 *Supra* 2.6. Tokens.
268 R. Thomas, 'Blockchain's incompatibility for use as a land registry: issues of definition, feasibility and risk', *European Property Law Journal* 2017 6(3), p. 361-390; Rod Thomas 'Blockchain's unsuitability for real property transactions' in S. Murphy & P. Kenna (eds) *eConveyancing and Title Registration in Ireland* (Clarus Press, Dublin, 2018; M. Barbieri en D. Gassen, 'Blockchain – can this new technology really revolutionize the land registry system?', presentatie World Bank, 20 -24 maart 2017, download op https://www.notartel.it/export/contenuti_notartel/pdf/Land_Poverty_Conference_Blockchain.pdf; Maria Kaczorowska, 'Blockchain-based Land Registration: Possibilities and Challenges', *Masaryk University Journal of Law and Technology* 2019/2, p. 339-360.
269 Zie over dit probleem N. Lazuashvili, A. Norta & D. Draheim (2019) 'Integration of Blockchain Technology into a Land Registration System for Immutable Traceability: A Casestudy of Georgia'. In: Di Ciccio C. et al. (eds) 'Business Process Management: Blockchain and Central and Eastern Europe Forum'. BPM 2019. *Lecture Notes in Business Information Processing*, vol. 361. Springer, Cham, p. 219-233.
270 *Supra* hoofdstuk 3, Toepassing: virtuele munten, 3.11. Veiligheid en risico.

tig bij virtuele valuta. In dergelijk geval kan niemand meer over het onroerend goed beschikken.
– Ingeval van faillissement of verjaring is degene die beschikkingsbevoegd is over het onroerend goed niet degene die bezitter is van de private sleutel. Hetzelfde geldt als de rechter levering beveelt of zelfs de levering uitspreekt met een constitutief vonnis.[271]
– Bij overlijden, fusie en overname is er juridisch een andere partij of meerdere partijen die eigenaar zijn, terwijl zij niet per se de beschikking hebben over de private sleutel.[272] Sowieso hebben gewone blockchains vooralsnog geen goede regeling voor gemeenschappelijke goederen.

Voor het eerste geval zou men nog kunnen verdedigen dat de eigenaar zijn sleutel beter moet beschermen, al zullen vermoedelijk maar weinig eigenaren blij zijn met het risico dat zij bijvoorbeeld hun huis door een simpele computerhack kunnen kwijtraken. Voor de andere gevallen lijkt de enige sluitende oplossing te zijn dat er een autoriteit is die zonder bezit van de private sleutel beslissingen kan nemen over het goed. In een publieke, *permissionless* blockchain is dit niet mogelijk, behalve als een meerderheid van de *nodes* wil meewerken aan een *fork* (wijziging van de blockchain), maar het ligt niet voor de hand dat *nodes* elk overlijdensgeval of elke rechterlijke uitspraak controleren en goedkeuren. Dit betekent dat voor een werkbare blockchainoplossing voor vastgoed het lijkt dat een autoriteit moet kunnen ingrijpen tegen de wil van de bezitter van de private sleutel.[273] Dat komt neer op een *permissioned* blockchain, maar dan verdwijnt wel het voordeel van *immutability* zonder controle door andere partijen. Dit voordeel van niet-wijzigbaarheid is momenteel echter onverenigbaar met de eisen die we juridisch stellen bij vastgoed.
Daarnaast zijn er nog andere praktische moeilijkheden op juridisch vlak. Hoe moet worden omgegaan met gemengde of gedeelde bevoegdheden en rechten van derden,[274] zoals aanwezigheid van beperkte rechten, hypotheek en beslag? In dergelijke gevallen mag de bezitter van de private sleutel immers niet als enige beschikken over het goed. Hoe moet daarnaast worden omgegaan met het in vervulling gaan van ontbindende en opschortende voorwaarden in een leveringsakte? Hoe moet worden omgegaan met de controle op de titel tot overdracht, namelijk de overeenkomst waaruit het recht op levering is ontstaan, en hoe houd je rekening met de wettelijke bedenktijd bij koop van onroerend goed?

271 B. Verheye, 'Real estate publicity in a blockchain world: a critical assessment', *European Property Law Journal* 2017 6(3), p. 441-476, par. 33.
272 B. Verheye, 'Real estate publicity in a blockchain world: a critical assessment', *European Property Law Journal* 2017 6(3), p. 441-476, par. 25-26.
273 Maria Kaczorowska, 'Blockchain-based Land Registration: Possibilities and Challenges" *Journal: Masaryk University Journal of Law and Technology* 2019/2 p. 350; N. Peiró & E. Martinez García, 'Blockchain and Land Registration Systems', *European Property Law Journal* 2017 6(3), p. 296-320.
274 Benito Arruñada, 'Blockchain's struggle to deliver impersonal exchange', *Economic Working Paper Series Working Paper* No. 1549, download op https://econ-papers.upf.edu/papers/1549.pdf.

Wat voorstanders van een blockchainoplossing voor ogen hebben, lijkt meestal een blockchain die zou leiden tot een volledig positief stelsel. In realiteit lijkt een blockchain die alles kan wat we momenteel maatschappelijk en juridisch voor ogen hebben, zoals bijvoorbeeld rekening houden met overlijden en belangen van derden, niet verder te kunnen gaan dan een negatief stelsel, en zelfs dan zal ingrijpen door een autoriteit mogelijk moeten zijn.
Een blockchainoplossing zou dan nog steeds zinvol kunnen zijn in de vorm van een *permissioned* blockchain in beheer van het Kadaster. Daarmee is dan ook geregeld wie het protocol van de blockchain beheert. In zo'n geval is er echter nauwelijks verschil met een gewone automatisering en de kadastrale registratie is al geautomatiseerd (*supra* 4.3.). Misschien zouden de toelatingscontrole tot het register en de kadastrale registratie echter wel verder geautomatiseerd kunnen worden in een blockchain. Dit zou bijvoorbeeld wel een koppeling met de rechterlijke macht en de burgerlijke stand vereisen om de authenticiteit van gerechtelijke uitspraken en overlijden te controleren.

## 4.5. Blockchain als vervanging van de notaris

Hiervoor is al aangegeven dat de rol van het Kadaster moeilijk vervangen kan worden door blockchain. De rol van het register en de kadastrale registratie vereisen immers dat er kan worden ingegrepen tegen de wil van de geregistreerde eigenaar in.
De rol van de notaris is een andere, die dichter aanleunt tegen het zorgdragen voor partijbelangen. Daardoor lijkt het gemakkelijker om dit door partijen zelf te laten doen, in dit geval via blockchain. Om te bepalen welke mogelijkheden hier zijn, gaan we eerst in op de verschillende functies van de rol van de notaris.
De notaris voert diverse controles en andere handelingen uit. De primaire rol van inschrijving van aktes in het register is uiteraard direct over te nemen in een blockchainoplossing: partijen verrichten die transactie dan zelf met behulp van hun private sleutel. De controles zijn voor een deel waarschijnlijk wel te automatiseren, zoals de controles op beslag en hypotheek. Dit geldt in het bijzonder voor simpele standaardtransacties, zoals de levering van een woning gefinancierd met een hypothecaire lening.
Er komen echter ook regelmatig ingewikkelder transacties voor. Denk aan een woning die eigendom is van diverse erfgenamen die over de hele wereld wonen en waarvan eventueel enkelen minderjarig zijn, de overdracht van een vastgoedportefeuille in eigendom van een conglomeraat waarbij complexe financieringsconstructies zijn gekozen, of de splitsing van een gebouw in appartementen. Deze transacties zijn waarschijnlijk niet allemaal vooraf te programmeren in standaardtransacties. Het gevolg is dat voor zulke transacties een dienstverlener of autoriteit nodig blijft. Bij blockchain zou dat dan een specialistische vastgoedblockchainprogrammeur kunnen zijn. Hij doet dan in feite hetzelfde werk als een gespecialiseerd vastgoednotaris, namelijk de bedoeling van cliënten correct vertalen in gedetailleerde acties en controles. Een potentieel voordeel zou zijn dat als er eenmaal een goed programma is gemaakt voor een

bepaald type transactie, deze controles daarna snel en goedkoop kunnen worden uitgevoerd.

Niet alle controles zijn echter gemakkelijk uit te voeren op een blockchain. De controle op identiteit is cruciaal om fraude uit te sluiten. Zoals hiervoor genoemd, is een blockchain hier bijzonder kwetsbaar voor door de mogelijke 'hack' van de private sleutel van de eigenaar. Verder is het ook belangrijk om te weten wie de wederpartij is. Om hieraan tegemoet te komen, lijkt het opnieuw nodig een *trusted third party* in te schakelen. Dit zou neerkomen op het behoud en de herijking van de rol van de notaris of een hiermee vergelijkbare tussenpersoon.

Controle op wilsbekwaamheid en begrip van de transactie kunnen evenmin goed door blockchain worden uitgevoerd. Betrokkenheid van belangen van derden kan tot op zekere hoogte wel op de blockchain plaatsvinden, als beperkte rechten bijvoorbeeld ook in het protocol worden opgenomen, maar het is niet duidelijk wat er moet gebeuren als de eigenaar en de derde het niet eens worden. Andere belangen van derden en algemene belangen, zoals controle op witwassen, zijn moeilijk of praktisch onmogelijk om in blockchain op te nemen.[275]

De rol van de notaris bij de financiële afwikkeling lijkt op het eerste gezicht echter wel relatief gemakkelijk om te laten overnemen door een blockchainprogrammeur die een smart contract maakt voor de transactie. Toch zijn er diverse nadelen. Vaak willen partijen geen openbaarheid over de financiële transacties. Bij een blockchainimplementatie van de financiering is er echter sowieso enige mate van openbaarheid, zoals de bedragen die immers op de blockchain moeten worden overgeboekt. Er is daarnaast een valutarisico bij het gebruik van virtuele valuta. Verder is het van belang dat het smart contract met alle relevante gevallen rekening houdt. Als dit niet goed is gebeurd, bestaat immers het risico dat de betalingen niet verlopen zoals de bedoeling is of zelfs dat het geld blijft 'vastzitten' in het contract omdat er niet kan worden voldaan aan de voorwaarden voor uitbetaling.[276] Er zijn ook nog meer lastige situaties in te beelden, zoals het geval dat de verkoper failliet is gegaan en daardoor niet meer bevoegd is het goed te leveren.

Diverse aspecten van de rol van de notaris zijn dus wel deels of geheel over te nemen door blockchain, maar dat geldt niet voor alle functies. Blockchain kan die functies niet allemaal even goed overnemen.

Voor de functies die een blockchain deels of geheel kan overnemen geldt evenwel dat de notaris nog steeds een rol kan hebben. Particulieren mogen bijvoorbeeld ook zelf een huis kopen of hun woning verbouwen, maar schakelen vaak toch een makelaar of aannemer in die hen voor fouten kan behoeden. Dat gebeurt dan op vrijwillige basis. Voor een deel van de functies van de notaris die alleen de partijen zelf raakt is verdedigbaar dat partijen mogen kiezen of ze het zelf willen doen of toch liever een deskun-

275 T.F.E. Tjong Tjin Tai, 'De blockchain als alternatief voor de notariële praktijk', in: F.W.J.M. Schols & B.C.M. Waaijer (red.), *Financiële zorgplicht van de notaris*, preadviezen KNB 2018, Den Haag: Sdu 2018, p. 99-135; M.I.W.E. Hillen-Muns, 'Digitalisering in het notariaat', *WPNR* 7202 (2018), p. 552-565.

276 Denk bijvoorbeeld aan het geval dat na het storten van de koopsom in het contract de private sleutel verloren raakt van een partij die toestemming moet geven voor uitbetaling.

dige willen inschakelen. Dat ligt anders voor de functies die belangen van zwakke partijen, derden of het algemeen belang raken.
Wat betreft het waarborgen van belangen van zwakke partijen zou een oplossing kunnen zijn dat er vaker gebruik wordt gemaakt van de juridische middelen om transacties terug te draaien op grond van vernietiging. Dat leidt echter wel tot extra kosten en belasting van de rechterlijke macht. Op dit moment fungeert de notaris als poortwachter voor zulke gevallen, hoewel niet altijd alles goed gaat. Bovendien is terugdraaien niet altijd effectief mogelijk, bijvoorbeeld als een onroerend goed in de tussentijd al is verkocht en geleverd aan een derde te goeder trouw.
Voor de belangen van derden is ook niet direct een goede oplossing voorhanden. De notaris moet nu zelf letten op de aanwezigheid van zulke belangen en deze correct in acht nemen. Een mogelijkheid zou zijn dat derden op de blockchainregistratie rechten en claims, zoals beslag en koopovereenkomsten (art. 7:3 BW), kunnen laten inschrijven met blokkerende werking, waarna de rechter hierover kan beslissen. Als derden dit rechtstreeks kunnen doen, is het risico van misbruik en *chicanes* echter groot doordat anonieme partijen effectief allerlei transacties kunnen blokkeren. Bovendien blijft een probleem dat derden dan actief moeten letten op transacties die hun belangen kunnen schaden. Het is de vraag hoe groot dit probleem in de praktijk zou zijn. Er kan in bepaalde gevallen sprake zijn van een problematische informatieasymmetrie.
Wat betreft het algemeen belang geldt dat dit op dit moment niet goed gewaarborgd kan worden bij een blockchainoplossing. In de discussie over blockchain wordt vaak juist vooropgesteld dat de overheid geen controle uitvoert op blockchaintransacties, waardoor dus witwassen moeilijk kan worden tegengegaan. Misschien is het mogelijk een technisch goede oplossing voor het tegengaan van ongewenste transacties te vervaardigen, maar in de blockchainindustrie is daar tot nog toe op dit vlak weinig gerealiseerd. Bovendien lijkt het erop dat hier geen algemene programmeerbare regel voor te vinden is. Bij het toezicht wordt gewerkt met een meldplicht die wordt gevolgd door een inhoudelijke controle. Zowel het vaststellen of er reden is voor een melding alsook de inhoudelijke controle schijnt tot op heden niet in een harde regel gevangen te kunnen worden. Eerder dan het verdwijnen of overbodig worden van de rol van een notaris of vergelijkbare figuur, zouden we bij de toepassing van blockchaintechnologie dus eerder evolueren naar een herijking van de rol van die tussenpersoon[277].

## 4.6. Andere toepassingen van blockchain

Op internet zijn vele voorbeelden te vinden van andere toepassingen van blockchain buiten de keten van registratie van onroerend goed. Het vastleggen van huurcontracten op een blockchain was onder meer een project van de gemeente Rotterdam, Deloit-

277 Dezelfde conclusie wordt bereikt in de EU Study on Blockchains – Legal, governance and interoperability aspects (SMART 2018/0038), https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038, par. 3.3.1.9.

te en het Cambridge Innovation Center Rotterdam,[278] alsook een project bij Merin.[279] Bij Rabobank was er een project om huurinformatie vast te leggen.[280] Eind 2019 is daarnaast een project gestart onder andere in Zuid-Limburg (Digital DeConstruction) voor de inzet van blockchain bij circulair bouwen om gegevens over materialen vast te leggen (het zogenaamde materialenpaspoort[281] of -tracing).[282] Andere mogelijke toepassingen zijn bijvoorbeeld de verdeling van gebruiksrechten en de regeling van complexe financiering.[283]

De notaris heeft bij dergelijke projecten geen wettelijk voorgeschreven taak. Zijn rol is daarom vooral een adviserende en wordt ook niet onmiddellijk ondermijnd door de inzet van blockchain. Veel van dergelijke initiatieven zijn vooral vormen van digitalisering en automatisering, in dit geval via blockchain, die nuttig kunnen zijn en weinig effect hebben op de rol van de notaris. Andere projecten kunnen potentieel nieuwe functionaliteiten bieden en helpen om transacties mogelijk te maken of efficiënter te laten verlopen. De laatste tijd worden geregeld projecten met blockchain aangekondigd, die vervolgens geruisloos verdwijnen wegens onvoldoende succes. Het is echter vaak lastig te achterhalen wat daar de redenen voor waren.

278 https://www.binnenlandsbestuur.nl/digitaal/nieuws/rotterdam-zet-huurcontracten-in-blockchain.9553081.lynkx.

279 https://merin.nl/nieuws/merin-en-legalthings-lanceren-blockchain-toepassing-vastgoed.

280 https://www.rabobank.nl/bedrijven/cijfers-en-trends/vastgoed/huurinformatie-vastleggen-via-blockchain/.

281 https://circulairebouweconomie.nl/wp-content/uploads/2019/09/Rapport-CBE-Verkenning-materialenpaspoort-Jonge-Honden-iov-RVO-sept-2019.pdf.

282 https://www.nweurope.eu/projects/project-search/digitaldeconstruction-advanced-digital-solutions-supporting-reuse-and-high-quality-recycling-of-building-materials/.

283 Zie bijvoorbeeld ook International Blockchain Real Estate Association, https://ibrea.info en J. Veuger, A Viable Real Estate Economy with Disruption and Blockchain, Lambert Academic Publishing, 2020.

# 5. Blockchainsmart

*'Whereas most technologies tend to automate workers on the periphery doing menial tasks, blockchains automate away the center. Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly.'*[284]

Vitalik Buterin, bedenker van Ethereum-smartcontractplatform

## 5.1. Introductie

Blockchain is een technologie die de afhankelijkheid van autoriteiten en intermediaire partijen reduceert en in sommige gevallen deze entiteiten overbodig maakt of op zijn minst hun rol herijkt. Het concept werd voor het eerst toegepast voor het transfereren van de virtuele munt bitcoin, wat toelaat om zonder banken waarde te transfereren over internet. De toepassingsmogelijkheden van de technologie reiken echter veel verder. Ze kan ingezet worden in onder meer de distributie- en transportsector, de overheidssector, de medische sector of bijvoorbeeld voor auteursrechten. Het hoogtepunt van de blockchainhype ligt nu weliswaar achter ons, maar dat neemt niet weg dat er heel wat bedrijven, consortia en overheden druk in de weer zijn met blockchain, al is het soms wat meer in de luwte.
Dit hoofdstuk gaat dieper in op een aantal toepassingsmogelijkheden, zonder daarbij exhaustief te zijn. Een blockchainnetwerk biedt collectief ondersteuning voor drie soorten acties, die normaliter een vertrouwde partij vereisen: het registreren van feiten, het transfereren van activa en het afdwingen van regels. In de praktijk is er vaak sprake van een combinatie.

### 5.1.1. *Registreren van feiten*

Met behulp van een blockchain kan de integriteit van gegevens beschermd worden, kunnen gegevens effectief en onweerlegbaar geregistreerd worden en is een correcte tijdstempel van het moment van registratie gegarandeerd, wat antedatering onmogelijk maakt. Ook zijn er garanties dat de registratie gebeurt door een entiteit die daartoe gemachtigd is, aangezien het mogelijk is om enkel gemachtigde entiteiten toegang te

284 https://lsc.org/gala/vitalik-buterin-1.

verlenen tot de blockchain. Hierdoor ontstaat dus vertrouwen in de correctheid van de geregistreerde gegevens. De technologie kan evenwel niet uitsluiten dat foutieve zaken in de blockchain geregistreerd worden.

Blockchain kan bijgevolg helpen de herkomst, de integriteit, de onweerlegbaarheid en de correcte datering van documenten te garanderen. We denken hierbij onder meer aan rijbewijzen, identiteitsgegevens, diploma's, notulen van gemeenteraden, gerechtelijke uitspraken, benoemingen, testamenten, verkoop- en oprichtingsakten. Het hoeft natuurlijk geenszins beperkt te blijven tot officiële documenten. Blockchain kan ook gebruikt worden om bijvoorbeeld de echtheid van nieuwsberichten te verifiëren in de strijd tegen *fake news*[285]. Ook zouden alle relevante documenten uit het strafdossier in een strafzaak bijvoorbeeld met behulp van blockchaintechnologie geregistreerd kunnen worden, zodat alle betrokken partijen kunnen nagaan of ze dezelfde documenten ter beschikking hebben vanuit een *equality of arms*-perspectief. Dit wil niet per se zeggen dat deze documenten zelf in de blockchain moeten worden bewaard. Vaak volstaat een cryptografische hash, een unieke digitale vingerafdruk van die documenten.

Een typisch scenario is dat slechts een beperkt aantal autoriteiten, zoals gemeentelijke overheden, notarissen of rechters, het recht krijgen om documenten te registreren met behulp van de blockchain en dat een grotere groep de door de blockchain gegarandeerde eigenschappen, zoals de integriteit van het document, verifieert. Het blijft wel de taak en de verantwoordelijkheid van de registrerende autoriteiten om de correctheid van wat ze in de blockchain registreren ook op voorhand te verzekeren. In dit scenario blijft er dus een cruciale rol voor bijvoorbeeld notarissen en het Kadaster. Het is dus niet zo dat blockchaintechnologie de tussenkomst van autoriteiten en het vertrouwen dat daarmee gepaard gaat volledig overbodig maakt. We vertrouwen er in dit scenario bijvoorbeeld nog steeds op dat die autoriteiten enkel correcte, gevalideerde informatie registreren.

Laat ons even kijken naar de mogelijkheid tot het registreren van een testament met behulp van de blockchain. Een notaris registreert het testament van een burger in de blockchain. Een paar jaar later wil de burger het testament wijzigen. De notaris registreert de nieuwe versie in de blockchain. In geval van betwisting biedt de tijdstempel uitsluitsel over welk van de twee versies nu geldig is. We zijn bovendien zeker dat het testament ongewijzigd is. In wezen is hier echter weinig verschil met de huidige werking van het Centraal Testamentenregister (CTR) waarin notarissen en kandidaat-notarissen bijhouden wie een testament heeft laten opmaken. In het CTR staat ook wanneer en bij welke notaris dat was. Notarissen kunnen namens de erfgenamen het register raadplegen en particulieren kunnen gratis schriftelijk navragen of de overledene een testament heeft. Het CTR geeft evenwel geen informatie over de inhoud van het testament. Informatie hierover is te vinden bij de notaris die het testament heeft opgemaakt. Het verschil is dat notarissen bij het CTR de rol van tussenpersoon spelen, terwijl dit bij een blockchainregister niet noodzakelijk het geval is. De meerwaarde van

285 A. Berman, 'Adblock Plus to Use Blockchain to Detect Fake News', *CoinTelegraph*, 14 juni 2018, https://cointelegraph.com/news/adblock-plus-to-use-blockchain-to-detect-fake-news.

een blockchain lijkt hier momenteel echter minimaal. Zowel in het heden als in de toekomst blijft vertrouwen cruciaal. Indien er om een of andere reden een moment zou komen in de toekomst dat burgers notarissen niet meer vertrouwen, dan zouden zij er wellicht de voorkeur aan kunnen geven om hun testamenten met behulp van een blockchain te registreren.
Het kan echter ook anders. De burger creëert bijvoorbeeld een nieuwe private sleutel en registreert het bijhorende pseudoniem bij zijn notaris, zodat die laatste dit pseudoniem kan koppelen aan de burger. Vanaf nu kan de burger op elk moment, zonder notaris, een nieuwe versie van zijn testament in de blockchain registreren. Bij overlijden zoekt de notaris het meest recente testament op dat onder dit pseudoniem geregistreerd werd. Dit scenario lijkt sterk op het eigenhandig (holografisch) testament, met dat verschil dat men door registratie van dit testament in de blockchain een vaste datum verkrijgt én dat bij overlijden steeds bekend zal zijn dat er een testament is. Onder het huidige recht is het ook al mogelijk om een eigenhandig (holografisch) testament in bewaring te geven bij de notaris die het registreert in het CTR. In dit geval is er dus een rol weggelegd voor een *trusted third party*. De meerwaarde van blockchain ligt hier dus opnieuw in het feit dat er geen centrale tussenpersoon vereist is. Aangezien we ervan uit mogen gaan dat de burger de notaris en het CTR vertrouwt, kunnen we ons evenwel afvragen of de blockchaintechnologie in dit concrete voorbeeld een grote meerwaarde zou bieden. Dit scenario vereist bovendien een sterke bescherming van de private sleutel. We moeten bijvoorbeeld vermijden dat een erfgenaam de sleutel van de burger kan ontvreemden en namens hem of haar een vals testament op de blockchain registreert. Ook moeten we vermijden dat een persoon die minder helder van geest is door anderen gemanipuleerd wordt om een nieuw testament te registreren zonder dat deze persoon zich daar goed en wel van bewust is (dat gevaar bestaat natuurlijk ook vandaag al bij een eigenhandig testament). Ook in dergelijk geval kan de notaris eventueel een belangrijke rol spelen.

### 5.1.2. *Transfereren van activa*

Voortbouwend op het registreren van feiten kunnen ook transacties zonder tussenpartij met behulp van een blockchain geregistreerd worden. Elke transfer van activa is dan een feit dat in de blockchain geregistreerd wordt. We maken een onderscheid tussen virtueel geld, immateriële activa en materiële activa.
We hebben al in hoofdstuk 3, Toepassing: virtuele munten gezien dat met behulp van blockchaintechnologie bitcoins en andere virtuele munten getransfereerd kunnen worden zonder intermediaire banken. Bij de tweede categorie, immateriële activa, denken we onder meer aan het registreren en het transfereren van auteursrechten[286, 287] en internetdomeinnamen[288]. Ook het lokaal verhandelen van elektriciteit en elektriciteits-

286 www.ascribe.io.
287 B. Lodewijks, 'Wordt Audius de nieuwe, verbeterde SoundCloud?', *Tech Pulse*, 10 augustus 2018, www.techpulse.be/nieuws/226965/wordt-audius-de-nieuwe-verbeterde-soundcloud.
288 https://namecoin.org.

certificaten, bijvoorbeeld voor groene stroom, is een vaak aangehaald voorbeeld. In dit geval registreert een intelligente meter elektriciteitsconsumptie en -productie in de blockchain[289]. Afhankelijk daarvan betaalt of krijgt de participant van het netwerk verhandelbare *tokens* (*supra* 2.6. Tokens), zoals virtueel geld of zelfs certificaten. Ook zijn al ticketsystemen op de blockchain uitgewerkt met het specifieke doel namaak en zwarte handel tegen te gaan[290]. Bij de derde categorie, materiële activa, denken we onder meer aan een blockchain om zakelijke rechten op onroerende goederen over te dragen. Dit komt hierna uitgebreider aan bod (*infra* hoofdstuk 4, Blockchain en vastgoed).

### 5.1.3. *Afdwingen van afspraken*

In het geval van Bitcoin is de voornaamste regel (afspraak) dat al uitgegeven virtuele valuta niet nog eens uitgegeven kunnen worden (*double spend*), terwijl de persoon in kwestie ze niet meer bezit. Welnu, dankzij *smart contracts* kunnen we dit principe ruimer toepassen en om het even welke set van afspraken laten afdwingen door het netwerk in plaats van te vertrouwen op een intermediair orgaan. Zo kunnen activa getransfereerd worden als aan bepaalde voorwaarden voldaan is. Denk aan het automatisch uitkeren van een vergoeding als je vlucht meer dan drie uur vertraging opgelopen heeft of het toekennen van subsidies indien voldaan is aan bepaalde voorwaarden. Dit alles wordt mogelijk met behulp van *smart contracts*, die in hoofdstuk 2 besproken zijn. Een *smart contract* is doorgaans een set toepassingsspecifieke regels, uitgedrukt in computercode. Eén blockchainnetwerk kan daarbij heel wat verschillende *smart contracts* bevatten.
Er zijn dus tal van toepassingsmogelijkheden voor blockchain. Het vervolg van dit hoofdstuk gaat dieper in op een aantal casussen: financiële transacties, identiteitsbeheer, herkomst en toeleveringsketen, aantoonbaarheidsdienst en het omzeilen van censuur. In het volgende hoofdstuk wordt vervolgens bekeken hoe compatibel blockchain is met de privacyregelgeving, in het bijzonder de Algemene Verordening Gegevensbescherming (AVG). Dat laatste is immers een belangrijk aandachtspunt bij het implementeren van blockchaintoepassingen.

## 5.2. **Casus financiële transacties**

Financiële instellingen waren de eerste die met blockchaintechnologie aan de slag gingen. Het huidige financiële systeem is erg complex, wat risico's en kosten met zich meebrengt. Financiële instellingen hopen met blockchain deze complexiteit aanzienlijk te kunnen reduceren door verschillende lagen van intermediatie door centrale tus-

289 M. Orcutt, 'How Blockchain Could Give Us a Smarter Energy Grid', *MIT Technology Review*, 16 oktober 2017, www.technologyreview.com/s/609077/how-blockchain-could-give-us-a-smarter-energy-grid.
290 J. Keane, 'Blockchain Startups Take on Ticket Touting, But Will They Gain Traction?', *Coindesk*, 30 juli 2017, www.coindesk.com/blockchain-startups-take-ticket-touting-will-gain-traction.

senpartijen te verwijderen[291]. Daarnaast wordt gehoopt dat blockchain voordelen brengt in gevallen waar momenteel verschillende financiële instellingen elk afzonderlijk transactiegegevens moeten bijhouden, maar het wel cruciaal is dat die verschillende gegevensbanken gesynchroniseerd blijven. Verschillende consortia van banken werden al opgericht om gezamenlijke blockchainprojecten uit te werken, zoals *Ripple* en *R3*. Morgan Chase heeft zelfs zijn eigen *permissioned* blockchaintechnologie ontwikkeld, genaamd *Quorum*.

De aandacht van de financiële sector voor blockchain komt uiteraard niet onverwacht. Bij het afhandelen van transacties van effecten, zoals onder meer obligaties en aandelen, bijvoorbeeld, zijn doorgaans heel wat partijen betrokken, waarbij centrale tussenpartijen optreden in meerdere stappen van een transactie. Er wordt gekeken naar blockchain om dit proces te verbeteren. Het potentieel wordt bevestigd in een gezamenlijk rapport van de Europese en de Japanse centrale banken[292]. De Wereldbank is niet alleen geïnteresseerd, maar heeft ondertussen zelfs al meer dan honderd miljoen dollar aan obligaties uitgegeven, onderliggend gebruikmakend van blockchaintechnologie[293]. Dit is slechts een fractie van de 50 à 60 miljard dollar aan obligaties uit die de Wereldbank jaarlijks uitgeeft, maar niettemin een significant bedrag. Arunma Oteh, de schatbewaarder van de Wereldbank, formuleert het als volgt: '*We believe that emerging technologies equally offer transformative yet prudent possibilities for us to continue to innovate, respond to investor needs and strengthen markets*'. De tijd nodig voor de afhandeling van transacties wordt gereduceerd van vijf dagen naar enkele seconden. Tegelijkertijd zijn de beloftes van transparantie en verlaagde transactievergoedingen nog niet gerealiseerd[294].

De financiële sector stoot momenteel evenwel op belangrijke uitdagingen als ze blockchaintechnologie probeert toe te passen. Volgens Ripple, dat nochtans zijn eigen virtuele munt heeft, is het onwaarschijnlijk dat banken in de nabije toekomst voor internationale betalingen zullen overschakelen op *distributed ledger technologie* (DLT), waar ook blockchain toe behoort. De redenen liggen niet alleen bij schaalbaarheid en privacy, maar ook bij flexibiliteit en de kost om bestaande systemen aan te passen[295]. Een ander product van Ripple, *xCurrent,* maakt geen gebruik van blockchain of DLT, maar onder meer Banco Santander en de Amerikaanse bankgigant PNC willen het wel in een productieomgeving gebruiken. Later kan dan eventueel alsnog overgeschakeld

291 J. Ito, N. Narula & R. Ali, 'The Blockchain Will Do to the Financial System What the Internet Did to Media', *Harvard Business Review*, 9 maart 2017, https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media.

292 ECB en Bank of Japan, 'Securities settlement systems: delivery-versus-payment in a distributed ledger environment', maart 2018, www.boj.or.jp/en/announcements/release_2018/data/rel180327a1.pdf.

293 M. Orcutt, 'The World Bank is still loving its blockchain-powered bonds', *MIT Technology Review*, 20 augustus 2019, https://www.technologyreview.com/f/614198/the-world-bank-is-still-loving-its-blockchain-powered-bonds/.

294 H. Sender, 'World Bank breaks ground with blockchain bond sale', *Financial Times*, 9 augustus 2018, www.ft.com/content/f99186b2-9bb5-11e8-9702-5946bae86e6d.

295 A. Irrera, 'Banks unlikely to process payments with distributed ledgers for now, says Ripple', *Reuters*, 13 juni 2018, https://uk.reuters.com/article/us-blockchain-ripple/banks-unlikely-to-process-payments-with-distributed-ledgers-for-now-says-ripple-idUKKBN1J92JG.

worden naar *xRapid*, dat onderliggend dan weer wel gebruikmaakt van de Ripple-blockchain. Ook SWIFT heeft samen met 34 banken stevig met blockchain geëxperimenteerd, meer bepaald in het kader van afstemming van nostro/vostro rekeningen. Daar luidde het evenwel in 2018: '*While the PoC [het prototype] proved a resounding success, just don't expect a working solution anytime soon*.'[296] Anderzijds zijn er verschillende blockchainbedrijven zoals *Ripple* en *LightNet* die op termijn maar al te graag marktaandeel van SWIFT willen veroveren in de markt van internationale financiële transacties.
Concluderend is er veel potentieel voor de financiële wereld, maar kan het volledige potentieel op dit moment nog niet gerealiseerd worden. De Russische centrale bank vatte het in mei 2018 goed samen door te stellen dat blockchaintechnologie nog moet verbeteren qua veiligheid en schaalbaarheid en dat de technologie nog onvoldoende volwassen is[297]. Tegelijkertijd is het een bijzonder snel evoluerende technologie.

## 5.3. Casus identiteitsbeheer

Het nagaan of iemand is wie hij of zij beweert te zijn, is een uitdaging die al eeuwen oud is. In de digitale wereld is het zo mogelijk een nog complexer gegeven, maar tegelijkertijd bieden nieuwe technologieën ook nieuwe mogelijkheden. In toenemende mate vragen burgers een vlotte digitale afhandeling van transacties en tegelijkertijd voldoende aandacht voor privacy. Het is dan ook een van de voornaamste doelstellingen van de nieuwe AVG, de Algemene Verordening Gegevensbescherming (*infra* hoofdstuk 6, Privacywetgeving), om de veiligheid en de confidentialiteit van persoonsgegevens te beschermen en de controle van die persoonsgegevens bij het individu te leggen. Van belang is tevens de eIDAS-Verordening[298] die een digitale interne markt tracht te realiseren. Met de verordening wordt beoogd rechtszekerheid en vertrouwen bij elektronische transacties en diensten te verhogen, zodat het onlineverkeer makkelijker en veiliger wordt. Het verplichte onderdeel van de verordening, namelijk inkomend verkeer, is bindend voor 'openbare instanties' (art. 6 eIDAS-Verordening). Hieronder vallen de staat, regionale of lokale overheden (*i.e.* gemeenten en provincies en waterschappen), publiekrechtelijke instellingen[299] en samenwerkingsverbanden bestaande uit één of meer van deze overheidsinstanties of één of meer van deze publiekrechtelijke instellingen, of een private entiteit die door ten minste één van deze autoriteiten, publiekrech-

296 'Adoption of DLT presents significant operational challenges for Swift member banks', *FinExtra*, 8 maart 2018, https://www.finextra.com/newsarticle/31787/adoption-of-dlt-presents-significant-operational-challenges-for-swift-member-banks/blockchain.
297 S. Das, 'Blockchain Tech Isn't Mature Enough Yet, Says Russian Central Bank Official', *CCN*, 28 mei 2018, www.ccn.com/blockchain-tech-isnt-mature-enough-yet-says-russian-central-bank-official.
298 Verordening nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, *Pb.L.* 28 augustus 2014, afl. 257, 73.
299 Dit is een instelling die valt onder de definitie in artikel 2, lid 1, punt 4 Richtlijn 2014/24/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten (art. 3, punt 8 eIDAS-Verordening).

telijke instellingen of verenigingen is gemachtigd tot het verlenen van openbare diensten[300]. Sinds 9 september 2018 moeten deze openbare instanties Europees erkende inlogmiddelen accepteren binnen de digitale dienstverlening. Een nationaal eID dient nu grensoverschrijdend erkend te worden.

Een digitale identiteit bestaat onder meer uit gegevens bevestigd door één of verschillende autoriteiten. Dergelijke gegevens kunnen we vinden op digitale certificaten zoals diploma's, vergunningen of rijbewijzen, maar ook bij de gemeenten. Gemeenten houden in de *Basisregistratie Personen (BRP)* persoonsgegevens van burgers bij, waaronder naam, geboortedatum, burgerservicenummer en adres. Daarnaast bestaat de digitale identiteit van een burger eigenlijk ook uit zijn of haar profielen op sociale media zoals Facebook, Twitter en Instagram en uit allerlei persoonsgegevens die elders digitaal bijgehouden worden.

Tegenwoordig zit de digitale identiteit van de burger verspreid over vele datasilo's zoals Facebook, het gemeentelijk BPR, overheidsadministraties, onderwijsinstellingen, banken, verzekeraars en ziekenhuizen. Dergelijke silo's zitten boordevol gevoelige persoonsgegevens en kunnen daarom doelwitten zijn voor cyberaanvallen. Een voorbeeld daarvan is de hack in 2017 op het kredietregistratiebureau *Equifax* waarbij gegevens van 145 miljoen Amerikanen gestolen werden[301]. Een tweede voorbeeld uit 2018 is de kwetsbaarheid van *Facebook*, waardoor hackers niet alleen toegang konden krijgen tot persoonsgegevens van 50 miljoen gebruikers, maar ook deze accounts konden overnemen[302].

Naast een veiligheidsrisico is het huidige model voor de burger bijzonder onpraktisch en onoverzichtelijk. Ten eerste is het bijna onmogelijk om te weten te komen welke gegevens waar bewaard worden, laat staan voor welke doeleinden ze gebruikt worden. Ten tweede is het beheer van de wachtwoorden op een veilige manier bijzonder onpraktisch. Ten derde kan de burger moeilijk selectief zaken over zichzelf prijsgeven. Om aankopen te doen, zoals vuurwerk en alcohol, is het voldoende om te bewijzen dat je meerderjarig bent, zonder dat je eigenlijk alle gegevens op je identiteitskaart, waaronder je exacte geboortedatum en naam, prijs moet geven. Ten vierde kan een burger zijn identiteit en data niet meenemen. Stel dat iemand Facebook verlaat en naar een alternatief sociaal netwerk verhuist, dan kan zij die identiteit, waaronder de vriendenlijst, die ze op Facebook opgebouwd heeft, niet meenemen.

Uit deze vier punten blijkt dat het bijzonder nuttig zou zijn om de controle over de persoonsgegevens terug te geven aan de burger. Dit is echter een complex probleem dat al tientallen jaren oud is. Met blockchain is er een hernieuwde interesse om deze uitdaging – het streven naar een *self-sovereign identity* – aan te gaan.

Er zijn dan ook heel wat experimenten wereldwijd om een deel van deze complexe uitdaging aan te pakken. Sommige van die initiatieven kijken daarvoor naar block-

300 Artikel 3, punt 7 eIDAS-Verordening.

301 D. Morris, 'The Equifax Hack Exposed More Data Than Previously Reported', *Fortune*, 11 februari 2018, http://fortune.com/2018/02/11/equifax-hack-exposed-extra-data.

302 Zie 'Facebook Security Breach Exposes Accounts of 50 Million Users', *The New York Times*, 28 september 2018, www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

chain als één van de puzzelstukken in dit verhaal. Op Europees niveau wordt getimmerd aan het ESSIF (European Self Sovereign Identity Framework)[303] dat van blockchain gebruik zal maken. *Self-sovereign identity* is tevens één van de speerpunten van de Dutch Blockchain Coalition en ook de TU Delft bijvoorbeeld werkt er intensief aan[304]. Anderzijds is ook het jonge *Solid*[305] project van Tim Berners-Lee, uitvinder van het World Wide Web, het vermelden waard, ook al maakt het geen gebruik van blockchain. De filosofie daarbij is dat elke burger één of meer 'potten' met persoonsgegevens beheert en zelf bepaalt wie toegang heeft tot welke persoonsgegevens. Solid wil zo een scheiding maken tussen de persoonsgegevens van de burger en de service waar de burger gebruik van maakt. Dit staat in schril contrast met de huidige aanpak waarbij een service, denk bijvoorbeeld aan Facebook, die een dienst aanbiedt, ook jouw data (bijvoorbeeld posts, comments, likes en foto's) controleert en beheert.
Hierna bespreken we een aantal blockchaininitiatieven rond digitale identiteit: een digitale identiteit voor vluchtelingen, diploma's, het selectief prijsgeven van basisinformatie en controle over verspreide persoonsgegevens. We ronden af met enkele bemerkingen rond het bredere vraagstuk van *self-sovereign identity*. Sowieso moet eerst het identiteitsverhaal stevig uitgebouwd zijn vooraleer kan worden overgegaan tot meer complexe blockchaintoepassingen. We spreken dan niet alleen over burgers, maar ook over ondernemingen en zelfs zaken zoals intelligente toestellen.

### 5.3.1. *Digitale identiteit voor vluchtelingen*

Artikel 6 Universele Verklaring van de Rechten van de Mens bepaalt dat eenieder, waar hij zich ook bevindt, het recht heeft als persoon erkend te worden voor de wet. In september 2015 hebben alle leden van de VN dan ook de *Sustainable Development Goals (2015-2030)* aangenomen met als een van de doelstellingen om tegen 2030 aan eenieder juridische identiteit toe te kennen, inclusief geboorteregistratie (target 16.9). Dit wordt een grote uitdaging, vooral bij de vele vluchtelingen. Problemen met betrekking tot identiteitsbeheer zien we inderdaad geregeld terugkomen in de context van vluchtelingen zonder papieren. In onze samenleving heeft men een grote kans te worden gemarginaliseerd zonder identiteitsbewijs. Men heeft in beginsel geen toegang tot de reguliere banen-, woning- en onderwijsmarkt, wat kansen ontneemt en mensen kwetsbaar maakt voor uitbuiting. Men kan geen verzekering afsluiten, noch een bankrekening openen, rijbewijs behalen, gsm-abonnement kopen en zelfs gezondheidszorg wordt moeilijk. Kan blockchain hier bijdragen aan een oplossing?
In Finland biedt de migratiedienst een prepaid-Mastercard aan die gekoppeld is aan een digitale identiteit op een blockchain, waar ook de financiële transactiegeschiedenis bijgehouden wordt. De eigenaar van de kaart hoeft dus niet eerst zijn identiteit en kre-

303 A. Doerk, *eSSIF: The European self-sovereign identity framework,* https://medium.com/@HodlHelper/essif-the-european-self-sovereign-identity-framework-4572f6875e12.
304 *Trustchains as next-generation blockchains*, TU Delft, https://www.tudelft.nl/en/technology-transfer/development-innovation/research-exhibition-projects/trustchain/.
305 *SOLID – Switch between storage and apps while taking the data along*, Solid, https://solidproject.org/.

dietgeschiedenis te bewijzen aan een bank om een rekening te kunnen openen[306]. Hij kan via het systeem ook geld ontvangen, wat een hindernis minder is bij het vinden van werk. Elke transactie wordt geregistreerd in een blockchain, wat de immigratiedienst toelaat om de inkomsten en de uitgaven van de kaarthouders te volgen en begeleiding op maat te voorzien. Er kwam echter kritiek op dit project, aangezien de transactiegeschiedenis ook tegen vluchtelingen gebruikt zou kunnen worden. De Finse migratiedienst geeft toe dat de bezorgdheden omtrent privacy terecht zijn, maar dat het gebruik van het systeem vrijwillig is en dat de identiteit van de vluchtelingen afgeschermd blijft[307].

Dit doet denken aan een blockchainexperiment in het Verenigd Koninkrijk in 2016, waarbij alle uitgaven van uitkeringsgerechtigde werklozen en mindervaliden op een blockchain zouden komen om zo hun financieel beheer te ondersteunen[308]. Het systeem zou bovendien het risico op fraude en vergissingen verminderen. Het experiment veroorzaakte heel wat commotie vanwege privacybezorgdheden, omdat het Departement voor Werk en Pensioenen (DWP) zou toelaten na te gaan of de uitkeringen wel degelijk voor bepaalde zaken gebruikt worden.

In het Finse, noch in het Britse verhaal is echter sprake van een *self-sovereign identity*, aangezien de burger geen controle heeft over zijn eigen persoonsgegevens.

Ten slotte is er een globale publiek-private samenwerking, in de vorm van een snelgroeiende start-up genaamd ID2020[309], die beoogt om het identiteitsvraagstuk van vluchtelingen op te lossen met een combinatie van blockchain en biometrie. Microsoft en Accenture bijvoorbeeld hebben in dit kader een toepassing ontwikkeld om vluchtelingen zonder papieren in staat te stellen zich met een digitale identiteit te identificeren[310].

### 5.3.2. *Diploma's*

In een tijdperk van globalisering, waarbij eenzelfde burger in verschillende landen kan studeren en werken, zou het een meerwaarde zijn voor de burger om steeds aan mogelijke toekomstige werkgevers de authenticiteit en integriteit van zijn diploma's – waar dan ook ter wereld behaald – te kunnen bewijzen. Voor de werkgever die de diploma's vereist, zou het een meerwaarde zijn indien fraude uitgesloten wordt. Het opvragen van een diploma aan een universiteit kan daarnaast trouwens een duur en langzaam

306 M. Orcutt, 'How Blockchain Is Kickstarting the Financial Lives of Refugees', *MIT Technology Review*, 5 september 2017, www.technologyreview.com/s/608764/how-blockchain-is-kickstarting-the-financial-lives-of-refugees.

307 T. Rayner, 'How Finland is Using the Blockchain to Revolutionise Financial Services for Refugees', *Reset*, 10 mei 2018, https://en.reset.org/blog/how-finland-using-blockchain-revolutionise-financial-services-refugees-05102018.

308 G. Plimmer, 'Use of bitcoin tech to pay UK benefits sparks privacy concerns', *Financial Times*, 12 juli 1016, www.ft.com/content/33d5b3fc-4767-11e6-b387-64ab0a67014c.

309 https://id2020.org.

310 E. Valgaeren & J.J. Linneman, 'Inleiding – Blockchain ontketend', *Computerrecht* 2017/250, 1.

proces zijn. Een blockchainbenadering zou dit alles kunnen stroomlijnen en vergemakkelijken voor de diplomahouder.
Theoretisch zou men dezelfde doelstelling ook kunnen bereiken met een gecentraliseerde benadering. Tot op heden is zo'n dienst er op Europees niveau niet, laat staan op internationaal niveau. Het is ook maar de vraag of landen snel geneigd zouden zijn om mee te gaan in een dergelijk verhaal, waarbij ze de gedeeltelijk de controle afstaan aan en afhankelijk worden van een externe dienst. Met een blockchainbenadering kunnen dergelijke gevoeligheden vermeden worden, mits op een correcte manier aangepakt. Een blockchainbenadering is trouwens niet het enige alternatief op een gecentraliseerde benadering.
Het gebruik van een generieke publieke blockchain zoals Bitcoin of Ethereum is niet aangewezen, onder meer omwille van het gebrek aan schaalbaarheid en controle. Daarom kan gekozen worden om, samen met een aantal partners, een nieuw blockchainnetwerk op te zetten. De Dienst Uitvoering Onderwijs (DUO) heeft in dit kader samengewerkt met Vlaanderen, meer bepaald met Informatie Vlaanderen, en Agentschap voor Hoger Onderwijs, Volwassenenonderwijs, Kwalificaties en Studietoelagen (AHOVOKS)[311]. De eindgebruikers, de diplomahouders en werkgevers, maken geen deel uit van het blockchainnetwerk[312]. Het prototype laat toe dat scholen en overheden diploma's toevoegen, dat burgers een overzicht hebben van al hun diploma's en met behulp van een soort toegangscode kunnen bepalen wie welke diploma's wanneer mag zien.
Er is echter nog werk aan de winkel op het vlak van privacy en confidentialiteit. Alle diplomagegevens – dus niet enkel de unieke *fingerprints* – worden immers onvercijferd op de blockchain bewaard en gedeeld door alle participanten in het blockchainnetwerk. Dit valt niet op een eenvoudige manier op te lossen zonder afbreuk te doen aan de functionaliteit. Dit toont het belang aan van *privacy by design*, een principe dat sterk benadrukt wordt in de AVG en dat inhoudt dat je al vanaf het ontwerp van je toepassing rekening houdt met privacybescherming.
Idealiter komt men in een Europese context overigens tot een pan-Europese diplomablockchain, die door overheden en onderwijsinstellingen collectief beheerd en veilig gehouden wordt. Alleen zo wordt voldoende rekening gehouden met de internationale dimensie die onze onderwijs- en arbeidssector bepaalt. Op Europees niveau wordt momenteel al intensief gewerkt aan een blockchaininfrastructuur waarin de lidstaten participeren. 'Onderwijscertificaten en diploma's' is een van de *core use cases* waar naar gekeken wordt bij de totstandkoming van deze infrastructuur en is ook een speerpunt van de Dutch Blockchain Coalition[313].

311 *Use case Diploma's: een betrouwbare oplossing voor Nederland, België en straks heel Europa, Dutch Blockchain coalition*, https://visie.dutchblockchaincoalition.org/usecases-diplomas/.
312 K. Daniels, 'Certified for Life—International exchange & authentication of diplomas via blockchain', *Medium*, 31 juli 2018, https://medium.com/wearetheledger/certified-for-life-international-exchange-authentication-of-diplomas-via-blockchain-4e947720edd9.
313 https://dutchblockchaincoalition.org/en/usecases/onderwijscertificaten-en-diplomas.

### 5.3.3. *Selectief prijsgeven van basisinformatie*

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties begon al in 2016 na te denken over het selectieve prijsgeven van persoonsgegevens met behulp van blockchaintechnologie. Hierbij wordt het gebruik van blockchain gecombineerd met andere, al wat oudere en complexere technologie, *zero-knowledge proofs* genaamd. Deze laatstgenoemde technologie laat het selectief prijsgeven van persoonsgegevens toe. De technologie laat meer bepaald toe om eigenschappen te bewijzen over een waarde, zonder verdere informatie over die waarde prijs te geven. Een burger kan bijvoorbeeld bewijzen volwassen te zijn zonder zijn exacte geboortedatum of andere persoonsgegevens prijs te geven. In de blockchainpilot 'financiële noodstop' of 'digitale datakluis'[314] kan een burger ten aanzien van het Centraal Justitieel Incassobureau tijdig betalingsonmacht signaleren zonder verdere informatie prijs te geven over die schulden, zodat mensen met schulden kunnen worden geholpen hun boetes te voldoen en niet nodeloos in de armoede belanden. Het is een beetje zoals het tonen van je identiteitskaart, maar met bepaalde delen afgedekt. Bovendien bieden complexere *zero-knowledge proofs*, genaamd *attribute-based credentials*, de mogelijkheid tot *onlinkbaarheid*: wanneer eenzelfde burger tweemaal niet-unieke zaken over zichzelf bewijst, kan niet afgeleid worden dat het over dezelfde burger gaat (*infra* 7.6. Beyond blockchain). Stel bijvoorbeeld dat een burger online een museumticket koopt. Om recht te hebben op korting bewijst de burger daarbij in Utrecht gedomicilieerd te zijn. Na het museumbezoek bewijst diezelfde burger in de museumshop meerderjarig te zijn, zodat ze een artistieke fles alcohol met een opdruk van Johannes Vermeer kan kopen. Wanneer het bewijs van domicilie en het bewijs van meerderjarigheid naast elkaar gelegd worden, is er geen manier om te weten te komen dat het over dezelfde persoon gaat.
Door een gebrek aan technische details kan echter niet afgeleid worden of die laatste eigenschap ook aanwezig is in het Nederlandse experiment. Om dezelfde reden is het moeilijk na te gaan in welke mate de oplossing voldoet aan de AVG. De CJIB blockchain-pilot financiële noodstop zou volgens advocaat Simon Sanders, AVG-conform zijn.[315] Wat sowieso wel duidelijk wordt, is dat blockchain een belangrijk element zou kunnen zijn in het bredere en complexe *self-sovereign identity*-verhaal, waarin de aandacht voor privacybescherming centraal staat.

### 5.3.4. *Controle over verspreide persoonsgegevens*

Bepaalde types gegevens over een burger kunnen verspreid zijn over verschillende locaties. Een voorbeeld daarvan zijn medische gegevens, die in vele landen bewaard worden door verschillende huisartsen, ziekenhuizen of ziekenhuisclusters. Dit is natuurlijk allesbehalve overzichtelijk voor de burger, die geen goed beeld heeft welke gegevens

314 *The financial emergency brake. CJIB app provides citizens with a GDPR-proof way to declare payment inability*, maart 2019, https://northsearegion.eu/media/9067/cjib-the-financial-emergency-brake.pdf.
315 *The financial emergency brake. CJIB app provides citizens with a GDPR-proof way to declare payment inability*, maart 2019, https://northsearegion.eu/media/9067/cjib-the-financial-emergency-brake.pdf.

over hem bijgehouden worden en wie toegang heeft tot welke gegevens. Dit alles zou geregeld kunnen worden via een collectieve blockchain, die uiteraard niet de gegevens zelf, maar wel de unieke *fingerprints* van de gegevens, de verwijzingen naar de opslaglocaties van die gegevens en de toegangsrechten registreert[316].

### 5.3.5. *Naar een internet voor identiteit?*

Er is een terechte interesse in het vraagstuk van een universele digitale – bij voorkeur *self-sovereign* – identiteit voor burgers, ondernemingen en zelfs objecten. Uit bovenstaande beperkte uiteenzetting blijkt ook dat er volop geëxperimenteerd wordt en er nog veel werk aan de winkel is. We zien ook dat het een complex vraagstuk is, waarbij zich naast organisatorische en technische kwesties ook juridische uitdagingen voordoen, vooral op het vlak van de bescherming van persoonsgegevens. Blockchain zou een belangrijke rol kunnen spelen in de ontwikkeling van dergelijke digitale identiteit, maar zal wel met andere technologieën gecombineerd moeten worden om dit te realiseren. Blockchain is maar één aspect van de oplossing.

Een veelbelovend project in dat kader is *Sovrin*, dat wil komen tot een universeel *self-sovereign identity*-netwerk. Het is al vele jaren mogelijk bepaalde zaken over je identiteit te bewijzen door middel van digitale certificaten. Dergelijke certificaten zijn echter duur en *top-down* gestructureerd, waarbij de entiteit helemaal bovenaan vertrouwd moet worden. Sovrin heeft de ambitie de kosten te verlagen, het vertrouwen in de mate van het mogelijke – bepaalde centrale autoriteiten blijven noodzakelijk – te distribueren en via het geven van incentives een rijker ecosysteem rond vertrouwen te creëren. Het bevestigen van de correctheid van gegevens zou automatisch financieel beloond worden en niet langer voorbehouden worden aan een beperkt aantal klassieke autoriteiten zoals de overheid. Er is daarbij sprake van een synergie tussen blockchain en geavanceerde *zero-knowledge proofs*. De Dutch Blockchain Coalition heeft eind 2018 een rapport[317] over Sovrin gepubliceerd, waarbij technische, juridische en veiligheidsaspecten bekeken werden. Volgens de Dutch Blockchain Coalition is de conclusie van het onderzoek '*dat Sovrin bewezen heeft een serieuze speler te zijn op het gebied van SSI [self-sovereign identity], maar dat het product nog niet volledig tot wasdom is gekomen en daardoor vooralsnog niet tot winnaar kan worden uitgeroepen*.' Bovendien zijn niet alle technische aspecten vrijgegeven, wat een analyse bijzonder moeilijk maakt. Het is wel hoopgevend dat autoriteiten in het domein van digitaal identiteitsbeheer en privacy in het project betrokken worden.

Een volwassen *self-sovereign identity* technologie ontwikkelen is belangrijk, maar dan begint het werk nog maar voor overheden die het willen aanbieden. Indien een land al over een sterk uitgebouwd systeem voor identiteitsbeheer en authenticatie van burgers beschikt, zal het minder geneigd zijn over te schakelen op nieuwe systemen die een

316 S. Friedman, 'Harnessing blockchain for electronic health records', *GCN*, 20 juni 2018, https://gcn.com/articles/2018/06/20/cdc-blockchain-ehr.aspx.

317 Dutch Blockchain Coalition. *DBC publiceert studie naar Sovrin*. 23 oktober 2018. https://dutchblockchaincoalition.org/nieuws/dbc-publiceert-studie-naar-sovrin.

sterk afwijkende benadering hebben. België bijvoorbeeld behoort op dat vlak tot de koplopers. Het heeft het centrale *Rijksregister* waar gegevens over burgers, zoals hun geslacht, geboortedatum en domicilieadres bewaard worden, alsook het unieke burgeridentificatienummer, genaamd het rijksregisternummer. Elke Belg beschikt over een elektronische identiteitskaart waarmee authenticatie en digitale handtekeningen mogelijk zijn en waarmee persoonsgegevens bewezen kunnen worden.
In Nederland is er evenwel tot op heden geen integraal landelijk persoonsregister, hoewel er daartoe wel – tientallen miljoenen euro's kostende– pogingen ondernomen zijn[318]. Persoonsgegevens van burgers (ingezetenen) worden bijgehouden in de Basisregistratie Personen (BRP): elke gemeente heeft een afzonderlijke BRP. Als iemand gaat verhuizen naar een andere gemeente, verhuizen de persoonsgegevens met diegene mee. Migratie, het verplaatsen van alle gegevens uit het bestaande systeem naar een nieuw systeem, is een erg complexe en dure aangelegenheid. Daarbij spelen niet enkel technische maar evenzeer juridische redenen die migratie naar een centraal platform moeilijk maken omwille van het beheer van die persoonsgegevens door de gemeenten. Indien Nederland (of de EU) dus zou beslissen om volledig over te stappen naar zelfbeheerde identiteiten in een blockchain, moet dit dus goed voorbereid worden en zullen aanzienlijke budgetten vereist zijn.

## 5.4. Casus herkomst en toeleveringsketen

Waar en in welke omstandigheden werd voedsel geproduceerd en getransporteerd? Waar en wanneer werd een auto geproduceerd? Waar komen de onderdelen vandaan? Was alles sociaal en ecologisch in orde bij de extractie van grondstoffen voor deze onderdelen? Is de auto achteraf correct ontmanteld? Welke weg heeft een container afgelegd en waar bevindt deze zich nu?
Dit zijn allemaal belangrijke vragen met betrekking tot verwerkingsketens van producten. Bij het beantwoorden van die vragen zou blockchaintechnologie een belangrijke rol kunnen spelen. Alle bedrijven betrokken in dergelijke ketens zouden op het moment van productie, verwerking of transport hun bijdrage in het proces kunnen registreren in de blockchain, die aldus de volledige geschiedenis bevat. Er kunnen uiteraard nog steeds foutieve zaken geregistreerd worden op de blockchain, maar dit wordt moeilijker. Bepaalde anomalieën in de blockchain door foute of frauduleuze registraties kunnen immers gedetecteerd worden. Achteraf sjoemelen en antedatering worden sowieso onmogelijk.
De consumentenbond deed een onderzoek naar voedselfraude en onderzocht 150 producten. Daaruit bleek dat in 21% van de gevallen gesjoemeld werd[319]. Onweerlegbare traceerbaarheid van de herkomst en route van producten zou welig tierende voedselfraude sterk kunnen terugdringen en vertrouwen kunnen creëren door het bieden van

318 Overigens zijn er wel andere bestanden waarin (praktisch) alle burgers zijn opgenomen, zoals bij de Sociale Verzekeringsbank.
319 N. Polderman, T. Cammelbeeck, H. Uitslag & L. de Gouw, *Onderzoek voedselfraude – gesjoemel met eten.* Consumentenbond, september 2016, https://www.consumentenbond.nl/acties/voedselfraude.

transparantie aan de consument. Bovendien zou het de voedselveiligheid ten goede komen. Het is dan ook niet verwonderlijk dat meerdere supermarktketens met blockchain aan de slag gaan.

Albert Heijn gebruikt de technologie al voor producten van haar huismerk, onder andere voor vruchtensap. Door het scannen van een QR-code kan de consument de volledige weg bekijken die het product afgelegd heeft. De vruchten werden bijvoorbeeld geplukt tussen augustus 2018 en januari 2019 op vijftien Braziliaanse plantages van multinational Louis Dreyfus en er verwerkt tot concentraat dat begin juni 2019 aangekomen is in de haven van Gent. Op 27 juli 2019 werd het door Refresco gebotteld, samen met water en vitamine C[320].

Internationaal kunnen we moeilijk naast de (private) *Food Trust*[321] blockchain van IBM kijken. Heel wat grote spelers in de voedseldistributiesector, zoals Walmart, Carrefour en Nestlé participeren erin. Het traceren van de herkomst van voedsel wordt dan ook gezien als één van de grote domeinen waar blockchain een toegevoegde waarde kan leveren.

Exact hetzelfde principe wordt toegepast voor het traceren van heel wat andere zaken. Sinds 2015 is het mogelijk[322] om de herkomst van diamanten te traceren, om zo de consument vertrouwen te geven dat het niet om bloeddiamant of synthetische diamant gaat. Ook IBM wil deze markt aanboren[323].

We zoomen even in op internationale handel. Bij het transporteren van een container van punt A naar punt B zijn vaak meer dan dertig partijen betrokken. Door de lage graad van digitalisering is het nog steeds een erg papierintensief en tijdrovend proces dat tot 50% van de totale kosten van het containervervoer opslorpt. Eenzelfde pincode wordt bovendien doorgegeven en hergebruikt door alle betrokken partijen gedurende het transport, wat niet erg veilig is. Maersk en IBM hadden daarom in 2018 een joint venture opgericht, wat resulteerde in het op blockchain gestoelde *TradeLens*[324] platform. Het heeft tot doel meer transparantie en eenvoud in het transport van goederen tussen grenzen en handelszones te bewerkstelligen, onder meer door het digitaliseren van de administratie betreffende import en export. Het wil een neutraal en open platform creëren dat een meerwaarde biedt voor alle betrokkenen, gaande van importeurs en exporteurs, havens en transporteurs tot douaneagentschappen.[325] Ondertussen participeren internationaal meer dan honderd bedrijven, waaronder grote spelers zoals MSC, CMA CGM en Hapag-Lloyd. Zo was de haven van Rotterdam was al betrokken bij een pilot waarbij vracht van Saoedi-Arabië naar Rotterdam geregistreerd werd op de blockchain.

---

320 https://www.businessinsider.nl/blockchain-nederland-2019/.

321 *IBM Food Trust*, IBM, https://www.ibm.com/blockchain/solutions/food-trust.

322 Everledger, https://www.everledger.io/.

323 R. Miller, 'IBM introduces a blockchain to verify the jewelry supply chain', *TechCrunch*, 26 april 2018, https://techcrunch.com/2018/04/26/ibm-introduces-trustchain-a-blockchain-to-verify-the-jewelry-supply-chain/.

324 TradeLens, https://www.tradelens.com/.

325 Zie 'Maersk and IBM to form joint venture applying blockchain to improve global trade and digitise supply chains', *Maersk*, 16 januari 2018, www.maersk.com/press/press-release-archive/maersk-and-ibm-to-form-joint-venture.

TradeLens lijkt dus een succes te worden. Nochtans reageerde de concurrentie in 2018 initieel negatief en stelden ze niet te gaan participeren. Een van de kritieken was dat het intellectueel eigendom in handen zou blijven van Maersk en IBM[326] en dat daardoor Maersk meer macht zou hebben in het platform dan haar concurrentie[327].
Ten slotte gaan we even naar de kledingindustrie. Ook deze sector heeft te kampen met een slecht imago, waarbij de productie geregeld plaatsvindt tegen lage lonen, soms bij onmenselijke werkomstandigheden. Kledingproductie kan bovendien ecologisch erg belastend zijn. De Zweedse modeketen H&M, die jaarlijks ongeveer 3 miljard kledingstukken verkoopt, biedt daarom sinds kort transparantie. In het persbericht[328] van H&M lezen we:

> *'Voor elk van onze kledingstukken delen we nu details zoals het productieland, leveranciersnamen, fabrieksnamen en adressen, evenals het aantal werknemers in de fabrieken. Bovendien kunnen klanten meer te weten komen over de materialen die worden gebruikt om een specifiek kledingstuk te maken. Door uitgebreide informatie te delen over waar onze kleding is gemaakt, maken we het klanten gemakkelijker om beter geïnformeerde keuzes te maken tijdens het winkelen.'*

H&M vermeldt nergens blockchain, wat doet vermoeden dat ze gebruikmaken van een traditionele, gecentraliseerde aanpak. Wellicht is een dergelijke aanpak technologisch eenvoudiger, maar een potentieel risico is dat de informatie vervalst kan worden en er dus een hogere graad van vertrouwen noodzakelijk is in tussenpersonen of centrale partijen.
Toch lijkt het er sterk op dat blockchain meer en meer gebruikt zal worden voor transparantie betreffende de herkomst en toeleveringsketen van allerlei producten. Vooral indien meerdere, met elkaar concurrerende partijen daarbij betrokken zijn, is blockchain veelbelovend.
Momenteel wordt de technologie in de toeleveringsketen echter nog niet echt grootschalig gebruikt. TradeLens claimt wekelijks 10 miljoen gebeurtenissen in de blockchain te schrijven (bijvoorbeeld 'container ABC123 is gearriveerd in de haven van Rotterdam'). Dat wil zeggen zeventien transacties per seconde. Dat is maar een fractie van de wereldwijde handel. De technologie en alles eromheen zijn echter nog in volle ontwikkeling en de situatie kan er dus binnen een paar jaar totaal anders uitzien. Hopelijk is er tegen dan een oplossing voor het capaciteitsprobleem waar blockchaintechnologie momenteel mee kampt.

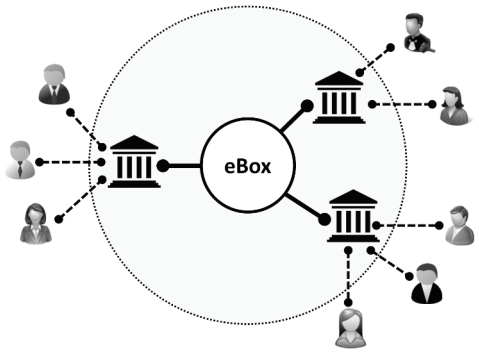
326 I. Allison, 'IBM and Maersk Struggle to Sign Partners to Shipping Blockchain', Coindesk, 26 oktober 2018, https://www.coindesk.com/ibm-blockchain-maersk-shipping-struggling.
327 O. Andersen & L. Vogdrup-Schmidt, 'Rivals reject blockchain solution from Maersk and IBM', ShippingWatch, 15 mei 2018, https://shippingwatch.com/carriers/Container/article10602520.ece.
328 'Press release: H&m first major fashion retailer to bring product transparency to scale', H&M, 23 april 2019, https://about.hm.com/news/financial-reports/2019/4/3275581.html.

## 5.5. Casus aantoonbaarheidsdienst

De sectie Onderzoek van Smals, de gemeenschappelijke IT-organisatie van de Belgische socialezekerheidsinstellingen, heeft in 2018 in detail een blockchaintoepassing uitgewerkt, waarbij zowel een uitgebreide analyse werd gemaakt, als een werkend prototype. Hierbij stonden privacy en veiligheid steeds centraal. De kernfunctie van deze blockchaintoepassing is het aantonen dat een bepaald document verstuurd of ontvangen is. Hierna volgen kort de krachtlijnen van deze toepassing.
Binnen de overheid creëert men in de eerste plaats eBox-platformen die gebruikt worden voor het uitwisselen van documenten tussen eindgebruikers[329]. Er zijn verschillende organisaties die elk een verschillend, niet-overlappend deel van de eindgebruikers vertegenwoordigen (zie figuur 11). Elke eindgebruiker wordt dus door exact één organisatie vertegenwoordigd. Wanneer Alice een bericht verstuurt naar Bob, is de flow als volgt:

1. Alice stuurt het bericht via haar organisatie naar de eBox.
2. Bob downloadt het bericht via zijn organisatie, die met de eBox verbonden is.

Alice en Bob maken daarbij gebruik van lokale software aangeboden door de organisatie waarvan ze deel uitmaken. De eBox dient te worden beschouwd als een gecentraliseerd uitwisselplatform voor documenten, waarop verschillende organisaties aangesloten zijn.




Figuur 11. eBox, organisaties en eindgebruikers.

Het is de bedoeling om een geavanceerde aangetekende zending te realiseren, waarbij we een bewijs ontvangen dat het document op een bepaald moment door Alice verstuurd werd en dat het op een bepaald moment door Bob ontvangen werd. Die bewij-

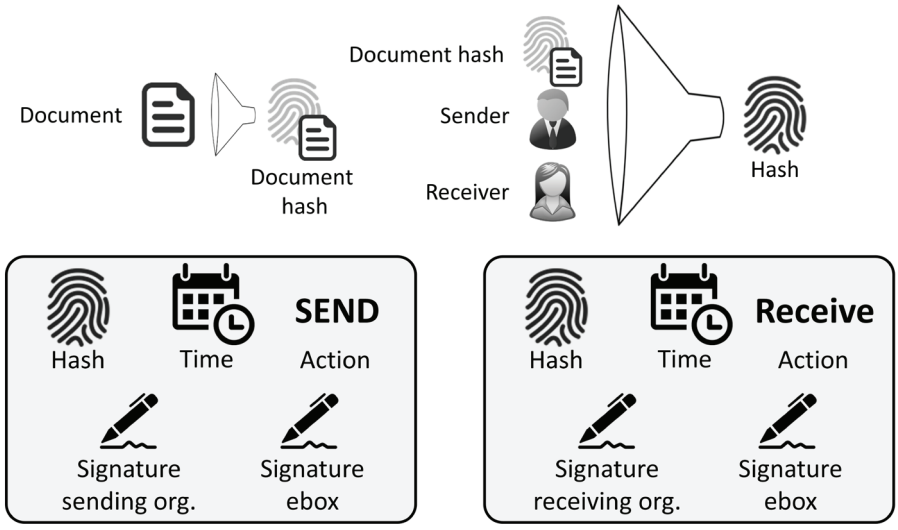
329 Er bestaan verschillende eBoxen. De aantoonbaarheidsdienst wil zo generiek mogelijk zijn en focust niet op een specifieke bestaande eBox.

zen moeten tientallen jaren bewaard worden. We kunnen erop vertrouwen dat de eBox dit correct zal doen, maar eigenlijk vertrouwen de eindgebruikers en organisaties de eBox daarvoor toch onvoldoende. Ook tussen de organisaties onderling bestaat een zeker wantrouwen. De eindgebruikers vertrouwen in beginsel wel hun organisatie. Een blockchainbenadering, waarbij de organisaties deel uitmaken van het blockchainnetwerk (de buitenste cirkel in figuur 11), lijkt dan ook een logische benadering.

In een ideale blockchainwereld zijn het de eindgebruikers zelf die direct participeren in het blockchainnetwerk. Dat vereist echter dat ze software installeren, draaiende houden en updates installeren wanneer nodig. Het vereist ook dat ze een private sleutel genereren en afdoende beschermen. Het vereist bovendien dat er een systeem is om te beheren wie wel of niet toegang heeft tot de blockchain, wat niet evident is met een grote variabele groep eindgebruikers. Eindgebruikers worden liever niet lastiggevallen met al het bovenstaande. Vandaar dat een benadering wordt voorgesteld waarin enkel de organisaties en de eBox participeren. Het gaat dan om een relatief kleine, stabiele set entiteiten die over de mogelijkheid beschikken om te participeren in het blockchainnetwerk. In deze benadering hoeft de eindgebruiker dus niet te weten dat er achterliggend een blockchain gebruikt wordt. De prijs is echter wel dat het vertrouwen gedecentraliseerd is onder een paar entiteiten, en niet is gedistribueerd onder de eindgebruikers.

Per document worden twee bewijzen gecreëerd: een bewijs dat een specifiek document afkomstig van Alice en bestemd voor Bob op een bepaald moment verstuurd werd naar de eBox en een bewijs dat het document ook op een bepaald moment ontvangen is. Zulk bewijs is eigenlijk een akkoord tussen de betrokken organisatie en de eBox. Het is een blockchaintransactie die door de twee partijen ondertekend wordt. De creatie van dit akkoord is bijgevolg een proces tussen de twee betrokken partijen.

Daarna wordt dit akkoord aan het blockchainnetwerk toegevoegd. Slechts indien de transactie door de eBox en een van de gekende organisaties ondertekend is, wordt het door het netwerk collectief aanvaard en komt het in de blockchain terecht, waar het onverwijderbaar is. Dit is een collectief proces tussen de betrokken organisaties. De eBox is in deze stap niet betrokken. Figuur 12 geeft vereenvoudigd de inhoud weer van zo'n akkoord. Eerst wordt de unieke *fingerprint* (cryptografische hash) van enkel het document berekend. De resulterende documenthash wordt nog eens gehasht, maar nu samen met de *identifier* van zowel de zender als de bestemmeling. Die finale hash komt in het bewijs terecht. Ten tweede bevat een bewijs de tijd waarop het akkoord gecreëerd is en ten derde de actie ('*verstuurd*' of '*ontvangen*'). Deze drie zaken worden ondertekend door zowel de eBox als de betrokken organisatie. Beide partijen ondertekenen pas als ze akkoord gaan met deze informatie. Het blockchainnetwerk verifieert vervolgens of het bewijs effectief ondertekend is door de eBox en een gekende organisatie en is op zich niet geïnteresseerd in de inhoud van het bewijs of akkoord. In dit geval bevat de blockchain dus geen persoonsgegevens, wat al een zorg minder is op het vlak van privacybescherming. Dit is immers een belangrijk gegeven gelet op het spanningsveld tussen de AVG en blockchain (*infra* hoofdstuk 6, Privacywetgeving).




Figuur 12. De inhoud (vereenvoudigd) van de SEND- en RECEIVE-bewijzen, die uiteindelijk op de blockchain terechtkomen.

Wat is de bewijskracht van een dergelijk bewijs? Er zijn drie niveaus, afhankelijk van de extra informatie die we bekomen.

1. Zonder extra informatie toont dit bewijs enkel aan dat een ongekend document op een gekend moment verstuurd of ontvangen werd door een ongekende eindgebruiker die aangesloten is bij een geïdentificeerde organisatie. Dit is wat de participanten in het netwerk sowieso te weten komen.
2. Wanneer we enkel over de documenthash en de *identifiers* van de afzender en bestemmeling beschikken, kunnen we bewijzen dat een ongekend document verstuurd door een geïdentificeerde afzender naar een geïdentificeerde bestemmeling op een bepaald moment verstuurd of ontvangen is. Dit komt functioneel in de buurt van zowel de klassieke papieren aangetekende zending als de metadata die telecomoperatoren juridisch verplicht zijn bij te houden.
3. Wanneer we naast de *identifiers* van de afzender en de bestemmeling ook nog het originele document hebben, kunnen we bewijzen dat exact dat document, verstuurd door een geïdentificeerde afzender en bestemd voor een geïdentificeerde afzender, op een gekend moment verstuurd of ontvangen is.

Een dergelijke granulariteit (*i.e.* de mate waarin detailgegevens aanwezig zijn) kan nuttig zijn. Ook zonder het document prijs te geven, kan immers een bepaalde activiteit bewezen worden.

Het bovenstaande is een vereenvoudigde voorstelling van de aantoonbaarheidsdienst. Zelfs voor deze relatief eenvoudige toepassing dient er goed nagedacht te worden over veiligheid om bijvoorbeeld te vermijden dat gevoelige gegevens, door middel van met-

adata op de blockchain, zouden kunnen lekken naar andere participanten in het netwerk of dat een hack bij één van de partijen verstrekkende gevolgen zou hebben. Een grondige analyse van de privacy en veiligheidsaspecten is dan ook steeds cruciaal. De blockchainfilosofie indachtig kunnen we nog een stap verder gaan en het bestaan van de eBox zelf, als centraal uitwisselplatform, aan de orde stellen. We moeten immers erop vertrouwen dat de eBox beschikbaar is, de documenten confidentieel behandelt en niet zelf gehackt wordt. Hoewel dit de eerstvolgende jaren wellicht onrealiseerbaar zal blijven, blijft het een interessante denkrichting.

## 5.6. Casus omzeilen censuur

Op een blockchain kan onverwijderbaar om het even welke data geregistreerd worden. Aan een bitcoin-transactie, bijvoorbeeld, kan de ondertekenaar – die we enkel kennen onder zijn pseudoniem – tot 80 bytes aan data toevoegen. Dit houdt echter grote risico's in en kan gevaarlijke en perverse gevolgen hebben. Zo bevat de Bitcoin-blockchain, naar verluidt, onder meer links naar afbeeldingen van kinderporno[330, 331].
Het toevoegen van data kan echter ook andere doeleinden dienen. In China registreren burgers bijvoorbeeld artikels in de Ethereum-blockchain om de censuur door de overheid te omzeilen. Burgers schrijven meer bepaald een klein bedrag naar zichzelf over waarbij aan de transactie een artikel toegevoegd wordt. Dit doen Chinese burgers onder meer om ongewenste intimiteiten kenbaar te maken en om de Chinese vaccinatiepolitiek aan te klagen[332].
In tegenstelling tot gecentraliseerde diensten zoals Facebook, kan een overheid niet zomaar toegang tot de servers of het datacenter blokkeren en kan ze niet van het bedrijf achter de gecentraliseerde dienst eisen de inhoud aan te passen of te verwijderen, of om bepaalde profielen te blokkeren. Bovendien kan een overheid de inhoud van beveiligde kanalen niet bekijken, wat het erg moeilijk maakt om Ethereum-verkeer te onderscheiden van ander verkeer. Ten slotte kan men de inhoud van de blockchain niet wijzigen.

## 5.7. Conclusie

In de periode 2016 tot 2018 werden heel wat blockchainprototypes gebouwd, die helaas veelal enkel geschikt waren voor de prullenmand. We zien dat evenwel dat zowel de technologie als de geesten langzaam aan het rijpen zijn. De periode van snel ontwikkelde wegwerpprototypes ligt in toenemende mate achter ons. Blockchaintechnologie

330 R. Matzutt, J. Hiller, M. Henze, J.H. Ziegeldorf, D. Müllmann, O. Hohlfeld & K. Wehrle, 'A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin', *Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC)*, Berlijn, Springer, 2018.

331 C. Kessler, 'Chinese Citizens Are Using Blockchain to Talk About Unsafe Vaccines', *Fortune*, 27 juli 2018, http://fortune.com/2018/07/27/china-blockchain-unsafe-vaccines.

332 E. Muzzy, 'How the Ethereum Blockchain Became a Tool in the Fight for China's #MeToo Movement', *Medium*, 16 mei 2018, https://medium.com/@everett.muzzy/how-the-ethereum-blockchain-became-a-tool-in-the-fight-for-chinas-metoo-movement-e4017b1acddd.

wordt stilaan selectiever en op een serieuzere, projectmatige wijze toegepast. Een van de auteurs (K. Verslype) is bijvoorbeeld betrokken bij het opzetten van een Europese blockchaininfrastructuur[333]. Bij bockchainprojecten realiseert men zich vaak – soms met vallen en opstaan – dat er toch nog een aantal hordes genomen zullen moeten worden. Desondanks biedt de technologie zeker mogelijkheden om de juridische en andere hordes te nemen.

333 European Blockchain Services Infrastructure (EBSI), European Commission, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi.

# 6. Privacywetgeving

## 6.1. Inleiding

Sinds 25 mei 2018 is de AVG, de Algemene Verordening Gegevensbescherming (AVG)[334], van toepassing. In het Engels staat deze bekend als de *GDPR*, de *General Data Protection Regulation*. Dit is een Europese verordening en heeft dus rechtstreeks werking in de EU-lidstaten. Het doel van de verordening is onder meer: '*het bieden van rechtszekerheid en transparantie, te voorzien in dezelfde wettelijk afdwingbare rechten voor natuurlijke personen in alle lidstaten en in verplichtingen en verantwoordelijkheden voor de verwerkingsverantwoordelijken en de verwerkers […]*'. Burgers verwachten in toenemende mate een vlotte digitale afhandeling van transacties en tegelijkertijd voldoende aandacht voor privacy. Het is dan ook een van de voornaamste doelstellingen van de AVG om de veiligheid en confidentialiteit van persoonsgegevens te beschermen en de controle van die persoonsgegevens bij het individu te leggen.
De AVG gaat uit van een aantal te respecteren basisprincipes. Bijzonder relevant in de context van blockchain zijn: behoorlijke en rechtmatige verwerking, het recht op rectificatie en vergetelheid, het recht op beperking van de verwerking en passende beveiliging. Vele blockchainprojecten hebben in de praktijk problemen met betrekking tot overeenstemming met de AVG. Michèle Finck, onderzoekster aan het Max Planck Instituut voor Innovatie en docente aan de University of Oxford, stelt[335]: '*There are many tensions and uncertainties between GDPR and blockchain and many blockchain projects are likely not compatible with GDPR*'. In wat volgt, wordt dit toegelicht[336]. Non-compliance met de AVG kan soms enkel vermeden worden door geen persoonsgegevens in de blockchain op te nemen, maar deze buiten de blockchain op te slaan of deze te pseudonimiseren of zelfs te anonimiseren vooraleer ze worden opgenomen[337]. In een private, *permissioned* blockchain blijkt het gemakkelijker om persoonsgegevens te verwerken

334 Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, *Pb.L.* 4 mei 2016, afl. 119, 1. Zie recentelijk EU Blockchain Observatory and Forum, *Thematic report Blockchain and the GDPR*, 16 oktober 2018, www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

335 EU Blockchain Observatory and Forum, *GDPR Workshop Report*, 8 juni 2018, www.eublockchainforum.eu/sites/default/files/reports/workshop_2_report_-_gdpr.pdf.

336 Voor het rapport van het R3-consortium, zie J. Moser, 'The Application and Impact of the European General Data Protection Regulation on Blockchains', *R3*, 15 februari 2017, www.r3.com/wp-content/uploads/2018/04/GDPR_Blockchains_R3.pdf.

337 Zie uitgebreid V.I. Laan & A. Rutjes, 'Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?', *Computerrecht* 2017/253.

in overeenstemming met het privacyrecht, aangezien er een soort van sturing of controlerende partij, een centrale verwerker aanwezig is.

## 6.2. Toepassingsgebied

Met betrekking tot het materieel toepassingsgebied is de AVG van toepassing op de geheel of de gedeeltelijk geautomatiseerde verwerking, alsmede de *verwerking* van *persoonsgegevens* (*infra* 6.3. Verwerking van persoonsgegevens) die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen[338]. De AVG is evenwel niet van toepassing op de verwerking van persoonsgegevens[339]:

a) bij activiteiten die buiten de werkingssfeer van het Unierecht vallen;
b) door lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, VEU (*i.e.* specifieke bepalingen met betrekking tot het gemeenschappelijk buitenlands en veiligheidsbeleid) vallen;
c) door een natuurlijk persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit;
d) door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

Met betrekking tot het territoriaal toepassingsgebied is deze verordening van toepassing op de verwerking van persoonsgegevens[340]:

1. bij de activiteiten van een *vestiging* van een verwerkingsverantwoordelijke of een verwerker in de Unie, *ongeacht of de verwerking al dan niet in de Unie plaatsvindt*;
2. van betrokkenen die zich in de Unie bevinden, door een *niet* in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking verband houdt met:
   a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of
   b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt;
3. door een verwerkingsverantwoordelijke die niet in de Unie is gevestigd, maar op een plaats waar krachtens het internationaal publiekrecht het lidstatelijke recht van toepassing is.

Voor toepassing van de AVG is het dus vooral van belang dat de *vestiging* van de verwerker of de verwerkingsverantwoordelijke in de Unie gelegen is (ongeacht of de verwerking zelf binnen de Unie plaatsvindt). De kwalificatie van participanten in een blockchain als verwerkers of verwerkingsverantwoordelijken is dus bijzonder belang-

338 Art. 2, lid 1 AVG.
339 Art. 2, lid 2 AVG.
340 Art. 3 AVG.

rijk om te bepalen of de AVG van toepassing is (*infra* 6.5. Rollen, relaties en verantwoordelijkheden).

## 6.3. Verwerking van persoonsgegevens

Artikel 4, lid 1 AVG definieert vervolgens persoonsgegevens als: '*Alle informatie over een geïdentificeerde of identificeerbare natuurlijk persoon („de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online-identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon*'. Het gaat dus om voor de hand liggende gegevens, zoals naam en adres, maar bijvoorbeeld ook afbeeldingen, locaties en videobeelden. Verwerking houdt op basis van artikel 4, lid 2 AVG het volgende in: '*een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens*'.

De AVG maakt een onderscheid tussen drie categorieën persoonsgegevens[341]. Ten eerste zijn er de *anonieme gegevens,* namelijk gegevens die niet te herleiden zijn naar een geïdentificeerde of identificeerbare natuurlijk persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is. Een voorbeeld zijn (bijvoorbeeld medische) anonieme statistische gegevens voor onderzoeksdoeleinden. De AVG is niet van toepassing op dergelijke anonieme gegevens. Ten tweede zijn er de *geïdentificeerde of identificeerbare persoonsgegevens,* die aan een natuurlijk persoon kunnen gekoppeld worden zonder bijkomende informatie. Een voorbeeld zijn medische records die telkens het burgerservicenummer van de patiënt bevatten. De AVG is ten volle van toepassing op geïdentificeerde gegevens. Ten derde zijn er de *gepseudonimiseerde gegevens*, die te koppelen zijn aan een natuurlijk persoon, maar enkel met behulp van additionele informatie die elders bewaard wordt. Een voorbeeld zijn medische records, waarbij de identificatiesleutels zoals het burgerservicenummer vervangen zijn door een unieke code en waarbij de tabel of sleutel die deze codes linkt aan burgerservicenummers elders wordt bewaard. De AVG blijft van toepassing op gepseudonimiseerde gegevens, maar sommige bepalingen zijn versoepeld, onder meer om wetenschappelijk onderzoek mogelijk te maken. Het verwijderen van de additionele informatie kan wel volstaan om gepseudonimiseerde gegevens om te zetten in geanonimiseerde gegevens.

Het kwalificatievraagstuk met betrekking tot de persoonsgegevens is dus bijzonder belangrijk. Om te bepalen of een natuurlijk persoon identificeerbaar is, moet rekening

341 Zie considerans 26 AVG.

worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken. Hiervoor moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen[342].

In een blockchaincontext is al snel sprake van gepseudonimiseerde gegevens. Alle gebruikers zijn inderdaad gekend onder een pseudoniem (*adres* in blockchainterminologie)[343]. Dit pseudoniem kan op verschillende manieren te herleiden zijn naar een natuurlijk persoon met behulp van extra informatie. Onderzoekers aan de Princeton University[344] vonden bijvoorbeeld een niet voor de hand liggende manier om dit te doen bij betalingen met virtuele munten:

> *'On most shopping websites, third party trackers receive information about user purchases for purposes of advertising and analytics. We show that, if the user pays using a cryptocurrency, trackers typically possess enough information about the purchase to uniquely identify the transaction on the blockchain, link it to the user's cookie, and further to the user's real identity'.*

Ook op afgeschermde (*permissioned*) blockchains is er doorgaans één partij of een aantal samenwerkende partijen die in staat zijn transacties te herleiden naar een geïdentificeerde entiteit die de transactie namens één van haar pseudoniemen ondertekend heeft. Voor zowel publieke als afgeschermde blockchainnetwerken valt een transactie ondertekend door een natuurlijk persoon dus onder de categorie van gepseudonimiseerde gegevens en is de AVG van toepassing.

Vercijferde persoonsgegevens zijn eveneens gepseudonimiseerde gegevens aangezien ze met externe informatie, namelijk de cryptografische sleutel, weer herleid kunnen worden naar een natuurlijk persoon. Het kan wel volstaan om de cryptografische sleutel te verwijderen om de cijfertekst, *i.e.* de vercijferde gegevens, om te zetten in anonieme gegevens. Aldus verdwijnt immers de mogelijkheid om de inhoud van de cijfertekst te lezen en dus om de cijfertekst te koppelen aan een natuurlijk persoon. Wat met de huidige middelen niet de decrypteren valt, is dat in de toekomst natuurlijk misschien wel, door de toename van rekenkracht, wiskundige doorbraken of de opkomst van kwantumcomputers.

342 Zie considerans 26 AVG.

343 Gebruikers van een blockchaintoepassing zijn niet per se natuurlijke personen. Natuurlijke personen maken wel het onderwerp uit van deze afdeling.

344 S. Goldfeder, H. Kalodner, D. Reisman & A. Narayanan, 'When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies', *Arxiv*, 2017, https://arxiv.org/pdf/1708.04748.pdf.

Ook het berekenen van een unieke *fingerprint* (cryptografische hash) van persoonsgegevens wordt gezien als een pseudonimiseringstechniek[345] en biedt op zich niet per se een afdoende bescherming van de persoonsgegevens. Het is bijvoorbeeld erg makkelijk voor een computer om uit een unieke *fingerprint* van een burgerservicenummer opnieuw het oorspronkelijke bsn te vinden door simpelweg voor alle nummers die de structuur van een bsn hebben (dat zijn er minder dan honderd miljoen, wat heel gemakkelijk is voor een computer), de unieke *fingerprint* te berekenen tot de juiste gevonden is.
Er moet dus telkens goed nagedacht worden over wat wel en niet op de blockchain bewaard wordt, welke additionele informatie gegevens op de blockchain kunnen leiden tot de identificatie van een natuurlijk persoon, wie die additionele informatie kent en hoe die additionele informatie beveiligd is (cfr. 'passende beveiliging' in de AVG). Soms kunnen zelfs op erg subtiele wijze persoonsgegevens afgeleid worden uit metadata op de blockchain. Indien er – al dan niet gepseudonimiseerde – persoonsgegevens op de blockchain bewaard worden, is de AVG van toepassing. Soms is de enige oplossing om geen persoonsgegevens in de blockchain op te nemen en deze buiten de blockchain op te slaan, of deze te pseudonimiseren of anonimiseren vooraleer ze worden opgenomen[346]. De kwalificatie van persoonsgegevens is dus bijzonder belangrijk.

## 6.4. Principes

Op basis van de artikelen 2, 3 en 4 AVG is de verordening dus al vrij snel van toepassing. Dit wil zeggen dat aan een aantal principes voldaan moet zijn. Een eerste principe in de AVG is behoorlijke en rechtmatige verwerking, waarvan de naleving onder de verantwoordelijkheid valt van de verwerkingsverantwoordelijke:
*Persoonsgegevens moeten*[347]*:*

a) *worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is;*
b) *voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt ('doelbinding');*
c) *toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ('minimale gegevensverwerking');*
d) *juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren;*

345 Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques', *PDP Journals*, 10 april 2014, 20, www.pdpjournals.com/docs/88197.pdf.
346 Zie uitgebreid V.I. Laan & A. Rutjes, 'Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?', *Computerrecht* 2017/253.
347 Art. 5, lid 1 AVG.

e) *worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is ('opslagbeperking');*
f) *door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ('integriteit en vertrouwelijkheid').*

Daarnaast is verwerking van persoonsgegevens alleen rechtmatig indien en aan ten minste een van de onderstaande voorwaarden is voldaan[348]:
a) *de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;*
b) *de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;*
c) *de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;*
d) *de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijk persoon te beschermen;*
e) *de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;*
f) *de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.*

Indien de vereiste grondslag voor de verwerking berust op *toestemming*, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens[349]. Hierbij heeft de betrokkene tevens te allen tijde het recht om op eenvoudige wijze zijn toestemming in te trekken[350]. Daarnaast is er het recht van rectificatie en vergetelheid**:**
– *De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen* (art. 16 AVG).
– *De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de ver-*

348 Art. 6, lid 1 AVG.
349 Art. 7, lid 1 AVG.
350 Art. 7, lid 3 AVG.

*werkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer […]* (art. 17 AVG).

Bovendien is er het recht op beperking van de verwerking**:**

– *De betrokkene heeft het recht van de verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen [onder bepaalde voorwaarden]* (art. 18 AVG).

Ten slotte zijn er nog het recht van inzage van de betrokkene (art. 15 AVG), het recht op overdraagbaarheid van gegevens (art. 20 AVG), het recht van bezwaar (art. 21 AVG), het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft (art. 22 AVG).
Ingevolge de opslagbeperking van persoonsgegevens in artikel 5, lid 1, sub e AVG moet de opslagperiode van persoonsgegevens tot een minimum worden beperkt en mag de opslag niet langer duren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt. Een basiseigenschap van een blockchain is echter net de onverwijderbaarheid van de gegevens. De opslagperiode kan dus niet beperkt worden, laat staan worden beperkt tot een strikt minimum. Dit lijkt tevens problematisch voor het recht op rectificatie, wat eventueel wel mogelijk kan gerealiseerd worden door de nieuwe, gewijzigde informatie toe te voegen aan de blockchain, en vooral het recht op vergetelheid evenals het recht op beperking van de verwerking. Dit vormt dan ook een van de belangrijkste drempels om een blockchain AVG-proof te maken. Aan dit probleem kan tegemoet worden gekomen door enkel gepseudonimiseerde gegevens op de blockchain te plaatsen die aan een natuurlijk persoon kunnen gekoppeld worden met behulp van aanvullende gegevens die elders bewaard worden. Door middel van procedures moet het daarbij echter wel mogelijk zijn om de additionele informatie te verwijderen die nodig is om die gepseudonimiseerde gegevens te herleiden naar een natuurlijk persoon. Op dat moment is er immers niet langer sprake van gepseudonimiseerde, maar van anonieme gegevens waardoor de AVG niet langer van toepassing is.
De verwerking door vele participanten op het blockchainnetwerk kan tevens een nadeel zijn in tegenstelling tot gecentraliseerde alternatieven die verwerking door minder participanten – en dus in zijn geheel minder verwerking – vereisen. Een voordeel bij blockchain is wel dat je gekend bent onder een pseudoniem, wat al een bepaalde mate van gegevensbescherming inhoudt. Indien de grondslag voor de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke er ook voor zorgen dat de betrokkenen uitdrukkelijke toestemming hebben gegeven voor de verwerking van hun persoonsgegevens en dat deze toestemming gemakkelijk kan ingetrokken worden. Dat laatste lijkt makkelijker realiseerbaar in een private, *permissioned* blockchain.
We moeten er ook rekening mee houden dat cryptografie die al vele jaren effectief is voor het versleutelen van informatie, dat in de toekomst misschien niet meer is. Er zijn immers evoluties gaande onder op het vlak van toenemende rekenkracht en sterke kwantumcomputers. Het kan bovendien niet uitgesloten worden dat aanvallen plaats-

vinden die de huidige cryptografische methodes verzwakken. Ook hierdoor kunnen beter geen vercijferde persoonsgegevens op een blockchain worden geplaatst.
Er moet dus goed nagedacht worden welke gegevens op een blockchain bewaard worden en welke technieken en procedures daarbij gebruikt worden. In het licht van de vereiste dataminimalisatie lijkt het beter dat zo weinig mogelijk persoonsgegevens op de blockchain worden opgeslagen. In een private, *permissioned* blockchain lijkt het gemakkelijker om partijen aan te duiden die persoonsgegevens moeten verwerken en kunnen participanten bij het toetreden van de blockchain gevraagd worden om uitdrukkelijk toe te stemmen met algemene voorwaarden met betrekking tot de verwerking van persoonsgegevens.

## 6.5. Rollen, relaties en verantwoordelijkheden

De AVG maakt een onderscheid tussen twee soorten relaties[351]. Ten eerste is er de relatie tussen een verwerkingsverantwoordelijke en de verwerker. De verwerkingsverantwoordelijke is '*een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*' (art. 4, lid 7 AVG). De verwerker is een '*natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt*' (art. 4, lid 8 AVG). Wanneer een e-commercebedrijf gegevens van zijn klanten laat analyseren door een ander bedrijf, is het eerste bedrijf de verwerkingsverantwoordelijke en de tweede de verwerker. De verwerker staat onder het gezag van de verwerkingsverantwoordelijke (art. 29 AVG). Verwerking is trouwens een bijzonder ruim gedefinieerde term. Daaronder vallen immers: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen (art. 4, lid 2 AVG).
Ten tweede kunnen ook relaties bestaan tussen verschillende verwerkingsverantwoordelijken onderling. In dat geval is er sprake van *gezamenlijke verwerkingsverantwoordelijken* (art. 26, lid 1 AVG): '*Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken*'. In dat geval moet in een onderlinge regeling vastgelegd worden wie verantwoordelijk is voor welke wettelijke vereisten onder de AVG. Uit die regeling moet blijken '*welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld*' (art. 26, lid 2 AVG).
In *permissioned* blockchainnetwerken is er ons inziens in beginsel sprake van gezamenlijke verantwoordelijkheden tussen de participanten in het netwerk en is er dus

351 Zie V.I. Laan, 'Privacy en blockchain: wanneer is er voor wie privacywerk aan de winkel?', *Tijdschrift voor Internetrecht* 2017/1, p. 4-11.

een onderlinge regeling nodig, waarin onder meer het doel en de middelen van de gegevensverwerking vastgelegd worden, wie de betrokkenen informeert, wie de wettelijke rechten aan de betrokkenen toekent (bijvoorbeeld het recht om gegevens te verwijderen en te corrigeren) enzovoort. De essentie van de regeling moet aan de betrokkene meegedeeld worden. Zo weet deze laatste bij welke partij een vraag tot verwijdering ingediend kan worden. Die partij stuurt de vraag dan door naar alle participanten, die vervolgens het nodige doen.

Indien de *nodes* als verwerkers zouden worden beschouwd, waarbij zij onder het gezag van de verwerkersverantwoordelijke de persoonsgegevens verwerken, dienen de verwerkingsverantwoordelijken met hen een verwerkersovereenkomst af te sluiten (art. 28, lid 3 AVG).

In het geval van een *permissionless* blockchainnetwerk, waarbij het participanten vrijstaat het netwerk te vervoegen of te verlaten, lijkt het ons het meest voorzichtig om de participanten allen als verwerkingsverantwoordelijken[352] te beschouwen die onafhankelijk van elkaar aan de verplichtingen van de AVG moeten voldoen. Ze moeten dan onafhankelijk van elkaar beoordelen of ze persoonsgegevens mogen verwerken, wat onder meer het publiek aanbieden ervan via de blockchain inhoudt. Indien persoonsgegevens buiten de EU verwerkt worden, is bovendien een grondige juridische evaluatie vereist van de in derde landen geboden bescherming (art. 44-49 AVG). In een volledig publieke blockchain is het dus vrijwel onmogelijk om te voldoen aan de AVG, aangezien zowel de participanten als hun locatie ongekend zijn. Het is dus bijzonder moeilijk om een adequaat niveau van gegevensbescherming te verzekeren.

Een rapport van de European Union Blockchain Observatory and Forum erkent dat het vaak moeilijk zal zijn – vooral bij *permissionless* blockchains – om de verwerkingsverantwoordelijken te identificeren en dat ook dit rapport bijvoorbeeld het debat over wie verwerkingsverantwoordelijken zijn, niet definitief kan beslechten[353]. Volgens het rapport moeten evenwel participanten die deelnemen aan de transacties voor persoonlijk gebruik, bijvoorbeeld om virtuele valuta te kopen, – in tegenstelling tot degenen die de blockchain gebruiken voor professionele doeleinden – waarschijnlijk niet als verwerkingsverantwoordelijken worden beschouwd. Zij zullen immers in beginsel vallen onder de uitzondering in artikel 2, lid 2, c AVG, op basis van welke de AVG niet van toepassing is op de verwerking van persoonsgegevens voor natuurlijke personen bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit. Volgens het rapport zal het tevens vaak aangewezen zijn om ontwikkelaars van het protocol die de '*open source*'-blockchaintechnologie ontwikkelen en onderhouden evenals *nodes* en *miners* in publieke, *permissionless* blockchains niet te beschouwen als verwerkingsverantwoordelijken[354]. Met betrekking tot degenen die smart contracts publiceren, blijft er

352 Zie in vergelijkbare zin S. Van Heukelom, J. Naves & M. Van Graafeiland, 'Whitepaper. Juridische aspecten van blockchain', *Pels Rijcken*, 28 september 2017, 9, www.pelsrijcken.nl/actueel/publicaties/whitepaper-juridische-aspecten-van-blockchain.

353 EU Blockchain Observatory and Forum, *Thematic report Blockchain and the GDPR*, 16 oktober 2018, 17, www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

354 *Ibid.*, 16.

onduidelijkheid. Het rapport stelt dat er op zich geen technologie is die sowieso AVG-conform is, maar dat steeds geval per geval moet worden gekeken naar de manier waarop de technologie wordt gebruikt. Het rapport erkent dat de AVG geenszins op alle vragen rond blockchain een duidelijk antwoord biedt.

## 6.6. Conclusie

De AVG en blockchain sluiten elkaar niet uit. Toch is er onmiskenbaar een spanningsveld tussen de twee. Michèle Finck formuleert dit als volgt:

> *'The GDPR was created for a world in which we have centralised data silos that collect, store and process data. Blockchains essentially decentralise all of those processes. So you certainly can't deny there's a tension between GDPR and blockchain, because they represent different visions of what the database is. As a result, it's very hard to figure out what a GDPR-compliant blockchain would be'*[355].

Enerzijds vrezen sommigen dat de AVG een rem zal zijn op de implementatie van blockchain in Europa. Anderzijds is het fundamenteel dat de privacy van burgers in de Europese Unie voldoende beschermd wordt. Het Europees Parlement denkt na over specifieke blockchainregulering, maar stelt, terecht, dat er opgelet moet worden om te snel wetgeving te maken voor een nieuwe technologie die nog niet goed begrepen wordt.

355 J. Kelly, 'Immutable ledgers meet European data protection', *Financial Times*, 12 april 2018, https://ftalphaville.ft.com/2018/04/12/1523503800000/Immutable-ledgers-meet-European-data-protection-.

# 7. Blockchain en gedistribueerd vertrouwen

*'You may be deceived if you trust too much, but you will live in torment if you do not trust enough'*[356].

Frank Crane, Amerikaans politicus en geestelijke eind 19de eeuw

Bij het horen van de term *gedistribueerd vertrouwen* zullen *believers* vol zelfvertrouwen over *blockchain* beginnen te praten. Wat is nu echter precies de relatie tussen blockchain en gedistribueerd vertrouwen? Hoe gedistribueerd is het vertrouwen in blockchainnetwerken? Bestaan er nog andere vergelijkbare technologieën? Dit hoofdstuk brengt hierover helderheid. Het gaat in op wat bedoeld wordt met gedistribueerd vertrouwen, bespreekt op conceptueel niveau wat blockchain wel en niet kan, doorprikt de mythe dat een blockchainbenadering per se een kostenreductie impliceert, gaat in op het spanningsveld tussen transparantie en confidentialiteit en bespreekt het blockchaintrilemma.

## 7.1. Gedistribueerd vertrouwen

Wat wordt bedoeld met de termen *gedistribueerd vertrouwen* of *distributed trust*? Dit concept betekent dat niet langer één enkele partij (toe)vertrouwd wordt om in een proces tot het gewenste resultaat te komen zonder ongewenste neveneffecten. Afhankelijkheden van één partij worden dus geëlimineerd of op zijn minst gereduceerd. Drie voorbeelden van dergelijke partijen zijn de volgende:

– Als een burger geld op een spaarrekening heeft staan, moet hij zijn bank vertrouwen, wat tijdens een bankencrisis[357] niet evident is.
– Als een burger gebruikmaakt van Facebook, vertrouwt hij er op dat de dienst beschikbaar is, afdoende beveiligd is en dat Facebook op een behoorlijke manier met zijn gegevens omgaat. Misbruiken zoals door Cambridge Analytica[358] zouden niet mogen voorvallen.

356 Geciteerd in *Business Education World* 1935, vol. 15, 172.
357 L. Laeven & F. Valencia, 'Systemic Banking Crises Database: An Update', *IMF working paper* 2012, nr. 163.
358 T. Adams, 'Facebook's week of shame: the Cambridge Analytica fallout', *The Guardian*, 24 maart 2018.

– Als een burger vastgoed bezit, vertrouwt hij er op dat dit correct door het Kadaster wordt geregistreerd en er ook in blijft staan. In Syrië bijvoorbeeld dreigen mensen door een nieuwe wet echter de aanspraak op hun woning en grond te verliezen[359].

In deze drie voorbeelden zijn burgers afhankelijk van respectievelijk een bank, een bedrijf en een overheidsdienst. De burgers moeten hen dus vertrouwen, of ze nu willen of niet. Blockchaintechnologie laat toe om niet langer afhankelijk te zijn van die ene partij, maar wel van een netwerk. Zolang de meerderheid van dat netwerk eerlijk is, loopt alles in beginsel zoals het hoort. Dat is gedistribueerd vertrouwen.
Er is een stelling uit de cryptografie die als volgt luidt: *Elke berekening mogelijk met een centrale autoriteit, is ook mogelijk zonder*'. Wat algemener geformuleerd, wordt dit: '*Alles wat met een centrale autoriteit gedaan kan worden, kan ook zonder die autoriteit gedaan worden*'. Bitcoin en blockchain hebben de verdienste dit idee te hebben gepopulariseerd. Dit betekent echter niet dat blockchain de enige en in alle gevallen zaligmakende oplossing is. Sterker nog, dit idee uit de cryptografie is gestoeld op een andere, oudere technologie genaamd *secure multiparty computation*. Blockchain is een specifiek technologisch concept dat bepaalde vormen van gedistribueerd vertrouwen mogelijk maakt, maar blockchain staat geenszins gelijk met volledig gedistribueerd vertrouwen.

## 7.2. Mogelijkheden en beperkingen van blockchain

Blockchaintechnologie laat toe om drie zaken zonder vertrouwde autoriteit te regelen:

1. *Het beschermen van data*
   Blockchain kan garanties bieden met betrekking tot de integriteit, de onweerlegbaarheid en de herkomst van gegevens. Ook is er achteraf geen antedatering of betwisting over het moment van registratie mogelijk. Denk bijvoorbeeld aan het registreren van diploma's en testamenten op de blockchain, maar ook aan het bijhouden van de geschiedenis van gebeurtenissen, bijvoorbeeld om transparantie te krijgen over de herkomst van voedsel.
2. *Het transfereren van activa*
   Bitcoin laat toe om, zonder bank, waarde (virtueel geld) uit te wisselen, maar blockchain laat in beginsel toe om elke vorm van waarde uit te wisselen, gaande van auteursrechten en domeinnamen tot diamanten en vastgoed. Eigenlijk wordt hier een simpele regel collectief door het netwerk afgedwongen: *de zender is ook de eigenaar van de activa die hij/zij wil transfereren*. Dit kan dus gezien worden als een specifieke, beperkte toepassing van punt 3 hierna.
3. *Het afdwingen van regels*

359 A. Van Es, 'Syrische vluchtelingen verliezen bij terugkeer mogelijk aanspraak op hun huis', *de Volkskrant*, 31 mei 2018, https://www.volkskrant.nl/nieuws-achtergrond/syrische-vluchtelingen-verliezen-bij-terugkeer-mogelijk-aanspraak-op-huis-en-grond~b303acf3/.

> In blockchainnetwerken wordt een set van regels collectief (gedistribueerd) afgedwongen. Met smart contracts kan dit ook voor willekeurige code. Geen enkele entiteit in het netwerk kan op zichzelf de correcte uitvoering ervan beïnvloeden. Een smart contract kan bovendien activa op de blockchain ontvangen, blokkeren en transfereren. Vaak komt het neer op het volgende: '*Indien aan voorwaarden A en B zijn voldaan, transfereer activa naar X*'.

Wat kan blockchain niet? Indien gegevens in de blockchain geregistreerd worden, kan het blockchainnetwerk niet de correctheid van deze gegevens verifiëren, tenzij alle data voor die verificatie zich al op de blockchain bevinden. Een blockchainnetwerk kan dus wel verifiëren of een bitcoin-transactie geldig is, maar weet niet of het huwelijkscontract of het diploma dat op de blockchain geregistreerd wordt, effectief rechtsgeldig is. Bij het gebruik van blockchain voor het transfereren van fysieke activa zal sowieso nog een partij vereist zijn die de link garandeert tussen wat op de blockchain geregistreerd staat en de reële wereld. Stel dat een smart contract je automatisch een bedrag uitbetaalt als je vlucht meer dan drie uur vertraging heeft, dan moet er informatie over de vluchten aan het smart contract aangeleverd worden via een orakel. Het smart contract kan evenwel niet nagaan of de aangeleverde informatie correct is. Foutieve input resulteert dus in foutieve output. *Garbage in, garbage out.*

Dezelfde informatie kan natuurlijk ook door verschillende partijen aangeleverd worden. Naarmate meer partijen onafhankelijk van elkaar hetzelfde zeggen, ontstaat een hogere graad van vertrouwen in de correctheid van die informatie. Stel dat wanneer je aan de gemeente aangeeft verhuisd te zijn, een overheidsdienst zou controleren of dit wel effectief zo is en er geen sprake is van fraude. Stel dat dit in de toekomst niet langer door de overheid zou gebeuren, maar door verschillende burgers en bedrijven: je buren bevestigen dat je daar effectief woont, alsook pakketbezorgers en nutsbedrijven. Het bevestigen van informatie gebeurt hier dus gedistribueerd, maar dit heeft op zich niets te maken met blockchain. Al deze entiteiten kunnen dit evengoed op een gecentraliseerde dienst aangeven. Het collectief valideren van extern aangeleverde informatie heeft dus op zich niets met blockchain te maken. Dit gebeurt al jaren bij *crowdsourcing*[360], waarvan Wikipedia het meest gekende voorbeeld is. Een collectieve validatie van externe informatie is dus in zekere zin complementair met blockchain.

Zonder vertrouwensissues is er op zich weinig reden om voor complexe blockchaintechnologie te kiezen. Dit betekent anderzijds niet dat bij een vertrouwensprobleem automatisch voor blockchain moet worden gekozen. Stel dat een aantal concurrerende partijen (banken) en een overheidsdienst moeten samenwerken en dat geen van deze partijen in het proces geëlimineerd kan worden. Indien de banken elkaar niet vertrouwen, is er een vertrouwensissue. Als ze echter alle de overheidsdienst vertrouwen, is er mogelijk een alternatief voor een blockchainbenadering op basis van traditionele tech-

360 Bij *crowdsourcing* maken organisaties (overheden, bedrijven, instituten) of personen gebruik van een grote groep niet vooraf gespecificeerde individuen (professionals, vrijwilligers, geïnteresseerden) voor consultancy, innovatie, beleidsvorming en onderzoek.

nologie, waarbij de banken dan wel afhankelijk worden van de overheidsdienst. In zo'n geval zou de overheid dus een centrale dienst kunnen aanbieden waar alle banken gebruik van maken. Door het bestaan van een vertrouwde instantie is een blockchainbenadering in dit geval niet onmiddellijk aangewezen.

Laat ons voor het tweede voorbeeld even teruggaan naar het beheer van diploma's met een blockchain (*supra* 5.3. Casus identiteitsbeheer, paragraaf 2. Diploma's). Het ontbreken van een Europese autoriteit voor het centraal beheer van diploma's impliceert niet dat blockchain de enige uitweg is. Indien elke lidstaat een diplomadienst aanbiedt met daarin de door haar onderwijsinstellingen uitgegeven diploma's, kunnen deze nationale diensten ook onderling communiceren. Om zijn diploma's te beheren, meldt een Nederlandse burger zich aan op de Nederlandse rijksdiplomadienst, die vervolgens op een klassieke digitale manier bilateraal informatie opvraagt aan de andere diplomadiensten. Aldus krijgt de burger een overzicht van zijn diploma's en eventueel de mogelijkheid die te beheren. Welke werkwijze de voorkeur geniet, zal uiteraard afhangen van de concrete vereisten.

Gedistribueerd vertrouwen betekent trouwens niet dat de noodzaak aan vertrouwen verdwijnt. We moeten er nog steeds op vertrouwen dat een meerderheid eerlijk is, er zich geen veiligheidskwetsbaarheden of bugs in de blockchainsoftware van de participanten of in het smart contract bevinden, het smart contract doet wat de makers beloven, de cryptografische assumpties waar alles op steunt correct zijn en blijven, de orakels hun werk correct doen, we onze private sleutel niet verliezen, het bedrijf dat onze virtuele munten beheert niet gehackt wordt, het netwerk niet verzadigd is wanneer we het willen gebruiken enzovoort. In tegenstelling tot wat soms beweerd wordt, is blockchain dus niet *trustless* of *vertrouwensvrij*. Er is nog steeds vertrouwen vereist, maar op een minder zichtbaar, abstracter en daardoor minder inzichtelijk niveau.

## 7.3. Kostprijs van gedistribueerd vertrouwen

Het reduceren van afhankelijkheden met behulp van blockchaintechnologie impliceert niet per se dat het proces ook goedkoper wordt, hoewel dat uiteraard wel mogelijk is. We verduidelijken dit aan de hand van drie voorbeelden.

Op het moment van schrijven waren de kosten[361] van een gemiddelde bitcoin-transactie teruggezakt tot ongeveer een halve dollar, na een piek op 22 december 2017 met een daggemiddelde van 55 dollar. Deze bedragen zijn onafhankelijk van het te transfereren bedrag. Om euro's in bitcoins om te zetten, wordt er trouwens nog een percentage[362] door de handelsplatformen aangerekend. Zelfs ten tijde van de piek was het gebruik van bitcoin echter soms nog goedkoper voor internationale transacties dan de klassieke weg. Lokaal een klein bedrag met Bitcoin uitgeven is, in vergelijking met de bestaande, gecentraliseerde systemen dan weer erg duur. Er zijn nog andere virtuele munten met lagere transactievergoedingen, maar Bitcoin is momenteel wel nog steeds de refe-

361 https://bitinfocharts.com/comparison/bitcoin-transactionfees.html.
362 https://en.bitcoin.it/wiki/Comparison_of_exchanges.

rentie. Bovendien gaat met het gebruik van Bitcoin een stevige ecologische kost gepaard (*supra* 3.5. Ecologische impact)[363].

Een tweede voorbeeld vinden we hier in Nederland. Door de Nederlandse gemeente Stichtse Vecht werd bekeken[364] of blockchain een meerwaarde kan bieden bij het aanvragen van een rolstoel. Daarbij zijn, naast de burger, het gemeentebestuur en verschillende zorgaanbieders betrokken. Ze maakten de vergelijking: wat als we dit regelen met behulp van een publieke blockchain, een afgeschermde (private) blockchain of een traditionele centrale database. Het resultaat is te zien in figuur 13. Een centrale database heeft een lagere infrastructuurkostprijs en complexiteit dan een afgeschermde blockchain. Ook wanneer gebruikgemaakt wordt van een publieke blockchain, is de complexiteit hoger volgens de tabel en zul je moeten betalen per actie. Die prijs fluctueert trouwens constant, afhankelijk van hoe verzadigd het netwerk is en hoe snel je de actie op de blockchain geregistreerd wilt krijgen. Het distribueren van vertrouwen leidt dus niet per se tot een afname van de kosten.

| | PUBLIC BLOCKCHAIN | PRIVATE BLOCKCHAIN | CENTRAL DATABASE |
|---|---|---|---|
| EIGEN SERVER NODIG | NIEMAND | GEMEENTE & ZORGLEVERANCIERS | GEMEENTE |
| CONTROLE DAT DATA NIET VERANDERT | GEMEENTE & ZORGLEVERANCIERS | GEMEENTE & ZORGLEVERANCIERS | GEMEENTE |
| € / ACTIE | HOOG | AFWEZIG | AFWEZIG |
| IMPLEMENTATIE COMPLEXITEIT | MIDDEL | HOOG | LAAG |
| BEVEILIGING TEGEN DATA MANIPULATIE | HOOG | VRIJ HOOG | NORMAAL |
| BEVEILIGING TEGEN DATA LEZEN | HOOG | HOOG | HOOG |
| AUDIT (WIE LAS DATA WANNEER) | ONMOGELIJK | ONWENSELIJK | STANDAARD |

Figuur 13. Vergelijking tussen de verschillende aanpakken voor de casus rond rolstoelgebruik op de blockchain door de Nederlandse gemeente Stichtse Vecht.

Laat ons evenwel afsluiten met een positief voorbeeld[365]. In Jordanië is er een *cash-for-food*-programma, georganiseerd door het WFP (World Food Programme) dat 110.000 Syrische vluchtelingen in Jordaanse vluchtelingenkampen helpt. Dankzij een oplossing die onder meer gebruikmaakt van blockchain zijn de transactiekosten, die voorheen naar lokale banken gingen, met 98% verminderd, aldus Houman Haddad, hoofd van

363 https://digiconomist.net/bitcoin-energy-consumption.

364 *Gemeente Stichtse Vecht – Rolstoelgebruik in Blockchain*, Blockchain pilots Dutch Government, Pilotronde 2, 2017, https://blockchainpilots.nl/.

365 R. Juskalian, 'Inside the Jordan refugee camp that runs on blockchain', *MIT Technology Review*, 12 april 2018.

de sectie *opkomende technologieën* binnen het WFP[366]. Alles hangt dus af van het concrete geval.
Samengevat komt het neer op het volgende. Alles wat mogelijk is met behulp van een blockchainbenadering is vanuit een puur technologisch standpunt op een efficiëntere en eenvoudigere manier te regelen met een gecentraliseerde benadering. Indien er echter geen geschikte partij is die de rol van centrale vertrouwde partij op zich kan nemen, of indien dit praktisch onhaalbaar of onwenselijk is of te grote risico's inhoudt, is een blockchainbenadering te overwegen.

## 7.4. Transparantie en confidentialiteit

Blockchain kan ons helpen om data collectief te beschermen en collectief regels af te dwingen. Kan blockchain dit echter zonder nadeel of is er toch een bepaalde prijs die we moeten betalen? Het verzoenen van enerzijds blockchain om vertrouwen te distribueren, en anderzijds confidentialiteit, bijvoorbeeld om de privacy van de burger te beschermen, is niet altijd een gemakkelijke evenwichtsoefening. Blockchaintechnologie is immers gebaseerd op transparantie, wat net in contrast staat met confidentialiteit.

### 7.4.1. *Beschermen van gegevens*

Een beperkte hoeveelheid ongevoelige (publieke) gegevens op een blockchain bewaren kan natuurlijk probleemloos. Op publieke, *permissionless* blockchainnetwerken zoals Bitcoin en Ethereum zul je daar wel een prijs voor betalen, uitgedrukt in de virtuele munt van het platform (bitcoin of ether). Je betaalt immers onder meer per byte. Sowieso moet worden opgelet met de hoeveelheid data die in de blockchain wordt gestopt, aangezien er niets uit verwijderd kan worden en de blockchain dus snel groot dreigt te worden.
Als gevoelige gegevens op de blockchain bewaard worden, kunnen meerdere participanten op het netwerk de data zien. Vercijfering is mogelijk, maar ook dat houdt risico's in. Vercijferde data kunnen in de toekomst misschien wel met behulp van kwantumcomputers[367] of een andere doorbraak gekraakt worden. Of misschien wordt de cryptografische sleutel gestolen of gaat die verloren. Een verschil met traditionele IT-infrastructuur is dat bij publieke, *permissionless* blockchainnetwerken er maar één schil van bescherming is, namelijk cryptografie. In een traditionele IT-infrastructuur heb je daarnaast ook andere schillen zoals toegangscontroles en firewalls.
Omwille van deze twee redenen, grootte en confidentialiteit, zal er veelal geopteerd worden om enkel een minimale hoeveelheid data, bijvoorbeeld een unieke *fingerprint*

366 C. Faulkner, 'How blockchain technology has changed the game for Syrian refugees in Jordan'. *The National*, 3 november 2019, https://www.thenational.ae/arts-culture/how-blockchain-technology-has-changed-the-game-for-syrian-refugees-in-jordan-1.932432.
367 D. Bouwmeester, A.K. Ekert & A. Zeilinger, *The physics of quantum information: quantum cryptography, quantum teleportation, quantum computation*, Berlijn, Springer, 2013.

van gegevens, op de blockchain te bewaren. Op die manier kunnen we nagaan of een document op de blockchain geregistreerd werd en wanneer en onder welk pseudoniem dit gebeurde, zonder dat de blockchain verdere informatie prijsgeeft. De data zelf kunnen dan vercijferd of onvercijferd elders bewaard worden door één of meerdere entiteiten.

We onderscheiden hierbij drie opties:

– Een eerste optie is dat de eindgebruikers van de applicatie of participanten in het blockchainnetwerk zelf de data bewaren. De burger is dan, als eindgebruiker, verantwoordelijk voor het bewaren van zijn diploma's, huwelijkscontracten, verkoopovereenkomsten enzovoort die in de blockchain geregistreerd staan. In dat geval zijn een goede back-up en beveiliging vereist. In het geval van diploma's kan iedere onderwijsinstelling, als participant in het netwerk, instaan voor het bewaren van de diploma's en notarissen zouden kunnen instaan voor het bewaren van notariële akten. Dat is gemakkelijker voor de burger, maar er wordt wel een afhankelijkheid in de vorm van een SPOF (*single point of failure*) gecreëerd. De server van de onderwijsinstelling of notaris bijvoorbeeld kan immers onbeschikbaar zijn of kan gehackt worden.
– Een tweede optie is dat de participanten in een blockchainapplicatie gebruikmaken van een gedeelde server met beveiligingsmechanismen zoals vercijfering en toegangscontrole. Bij blockchain is het echter net in beginsel de bedoeling om centralisatie te vermijden. Daarnaast leidt een dergelijke hybride oplossing tot hogere kosten. Toch kan een dergelijke oplossing noodzakelijk zijn om in overeenstemming te zijn met regulering. Denk daarbij in de eerste plaats aan de Algemene Verordening Gegevensbescherming (AVG). Dankzij vercijfering is het overigens niet per se nodig dat de centrale server zelf toegang heeft tot de gegevens. Het vereiste vertrouwen in de centrale server kan dus beperkt blijven.
– Een derde optie is dat de gegevens nog steeds – al dan niet vercijferd – door meerdere, participanten, maar wel buiten de blockchain, bewaard worden. In tegenstelling tot data in de blockchain hoeven deze data niet tot het einde der dagen bewaard worden en hoeft niet elke participant alle informatie te bewaren. Dit versoepelt de vereisten naar opslag toe aanzienlijk.

De gekozen optie zal afhangen van applicatie tot applicatie. Telkens zal gezocht moeten worden naar het juiste evenwicht. Soms zullen daarbij concessies gedaan moeten worden. Verder moet vermeden worden dat gevoelige gegevens afgeleid kunnen worden uit de metadata op de blockchain.

### 7.4.2. *Afdwingen van regels*

Blockchain laat toe om collectief regels te valideren. Bij een transactie van virtueel geld is dit beperkt tot: '*Is de zender ook de eigenaar van de activa die hij wil transfereren?*' Bij smart contracts kunnen die regels ook complexer zijn. Collectief valideren impliceert ook dat meerdere entiteiten toegang hebben tot dezelfde gegevens om aldus de valida-

tie te kunnen doen. Voor een smart contract dat automatisch belastingen int, zou dit dus betekenen dat meerdere entiteiten toegang hebben tot alle relevante belastinggegevens. Dit is meteen ook een achilleshiel van blockchain. Het uitschakelen van de centrale autoriteit betekent dat we meerdere participanten toegang geven tot potentieel gevoelige gegevens. We moeten hen dus vertrouwen deze gegevens niet te misbruiken. In het geval van een afgeschermd blockchainnetwerk is het aantal entiteiten met toegang tot de gegevens weliswaar beperkt en kunnen er contractuele afspraken gemaakt worden, maar moeten we er nog steeds op vertrouwen dat de gegevens niet misbruikt worden en dat de participanten niet gehackt worden.

Op de blockchain zijn we gelukkig niet gekend onder onze echte naam (of burgerservicenummer), maar onder een pseudoniem (adres). Helaas is dit een noodzakelijke maar onvoldoende vorm van bescherming. Bij een relatief eenvoudige toepassing, het transfereren van virtueel geld, zijn al diverse deanonimisatieaanvallen gepubliceerd[368, 369]. Naarmate een applicatie complexer wordt, en meer gegevens verwerkt worden, stijgt ook de kans dat deze gegevens door een aanvaller aan een burger (of bedrijf) gekoppeld kunnen worden. De AVG blijft dan ook – terecht – van toepassing op gepseudonimiseerde persoonsgegevens.

Er wordt gelukkig wel onderzoek gedaan om het ongewenst toegankelijk maken van informatie naar onbevoegden te verminderen. Een voorbeeld hiervan is het in 2016 gelanceerde *Zcash*[370], dat dankzij het gebruik van geavanceerde cryptografie erin slaagt om bij transacties van virtuele munten zowel het adres van de zender, het adres van de ontvanger, alsook het getransfereerde bedrag te verbergen, zelfs voor de validatoren. Dit klinkt langs de andere kant natuurlijk ook fantastisch als je criminele intenties hebt. Toch staat hier een prijs op. Daar waar een gemiddelde transactie in Bitcoin zowat 300 bytes groot is en in enkele milliseconden gecreëerd kan worden – de registratie op de blockchain buiten beschouwing gelaten –, wordt dit bij Zcash 2.000 bytes en enkele tientallen seconden op een typische desktop-pc, aldus het R3-consortium[371]. Bovendien is dit enkel een oplossing voor één specifieke toepassing van blockchain, namelijk het transfereren van virtuele munten.

De voorgestelde oplossing kan niet zomaar geëxtrapoleerd worden naar andere toepassingen, laat staan naar een generieke technologie zoals blockchaingebaseerde smart contracts. *Permissioned* blockchaintechnologieën zoals *Quorum*[372] en *Hyperledger Fa-*

368 M. Fleder, M.S. Kester & S. Pillai, 'Bitcoin transaction graph analysis', *Arxiv*, 2015, https://arxiv.org/pdf/1502.01657.pdf.

369 S. Goldfeder, H. Kalodner, D. Reisman & A. Narayanan, 'When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies', *Arxiv*, 2017, https://arxiv.org/pdf/1708.04748.pdf.

370 E.B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer & M. Virza, 'Zerocash: Decentralized anonymous payments from bitcoin' in '2014 IEEE Symposium on Security and Privacy', *IEEE*, 2014, 459-474, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6956581.

371 D. Yang, J. Gavigane & Z. Wilcox-O'Hearn, 'Survey of Confidentiality and Privacy Preserving Technologies for Blockchains', *R3*, 2016, www.r3.com/wp-content/uploads/2017/06/survey_confidentiality_privacy_R3.pdf.

372 'Quorum – Advancing Blockchain Technology', *J.P. Morgan*, www.jpmorgan.com/global/Quorum.

*bric*[373] laten wel toe dat een contract maar door een beperkt aantal personen of zelfs door enkel de betrokkenen gezien en uitgevoerd kan worden, maar dan is de graad van distributie natuurlijk minder groot. Bovendien blijkt de benadering in de praktijk tot op heden niet steeds even werkbaar, zoals blijkt uit experimenten door SWIFT[374]. Ook volgens Ripple, één van de toonaangevende spelers, is het onwaarschijnlijk dat banken in de nabije toekomst zullen overschakelen op *distributed ledger*-technologie, waar ook blockchain toe behoort. De voornaamste redenen zijn schaalbaarheid en privacy[375].
Heel wat pogingen om de confidentialiteit en de privacy in blockchaintoepassingen te verbeteren, zijn dan ook toepassingsspecifiek. Kristof Verslype, coauteur van dit boek, werd hier al in 2016 mee geconfronteerd bij het bouwen van een blockchainprototype voor het verwerken van medische voorschriften. De uiteindelijke oplossing voldeed aan strenge privacy- en confidentialiteitsvereisten. Daarvoor was wel een aanzienlijke schil cryptografie vereist, wat de complexiteit, en dus ook de kosten, aanzienlijk verhoogde. Naarmate een smart contract beslissingen moet nemen op basis van een rijkere set gegevens, wordt het moeilijker de identiteit van de betrokken burger of organisatie afdoende te beschermen.
Samengevat komt het gebruik van blockchain voor het afdwingen van regels vandaag met een prijs. Ofwel hebben meerdere partijen toegang tot bepaalde, mogelijk gevoelige gegevens, ofwel gebruik je complexe, vaak op maat gemaakte oplossingen, die bovendien een significante impact kunnen hebben op zaken zoals efficiëntie en schaalbaarheid. Ook de graad waarin het vertrouwen gedistribueerd is, kan hieronder lijden. Dergelijke oplossingen op maat zijn dan ook niet altijd mogelijk of wenselijk.

### 7.4.3. *Conclusie*

De volgende tabel geeft samenvattend een aantal mitigerende maatregelen en hun consequenties.

373 'Hyperledger Fabric – A Blockchain Platform for the Enterprise', *Hyperledger Fabric*, https://hyperledger-fabric.readthedocs.io.
374 Zie 'Adoption of DLT presents significant operational challenges for Swift member banks', *Finextra*, 8 maart 2018, www.finextra.com/newsarticle/31787/adoption-of-dlt-presents-significant-operational-challenges-for-swift-member-banks.
375 A. Irrera, 'Banks unlikely to process payments with distributed ledgers for now, says Ripple', *Reuters*, 13 juni 2018, https://uk.reuters.com/article/us-blockchain-ripple/banks-unlikely-to-process-payments-with-distributed-ledgers-for-now-says-ripple-idUKKBN1J92JG.

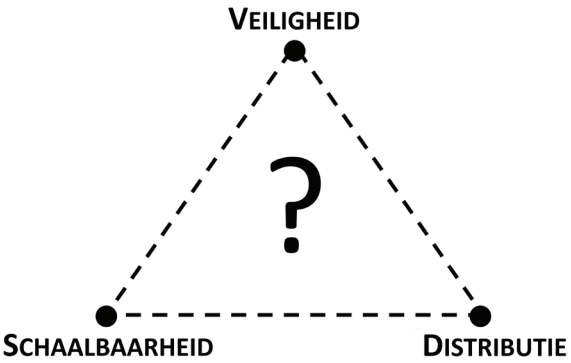
| MITIGERENDE MAATREGELEN | CONSEQUENTIES |
|---|---|
| *Pseudoniemen* | ▶ Deanonimisatierisico<br>▶ Vaak noodzakelijke maar onvoldoende maatregel |
| *Minder data on-chain* | ▶ Minder regels collectief gevalideerd<br>▶ Mogelijks lekt informatie via metadata<br>▶ Data moeten elders bewaard worden |
| *Minder participanten toegang tot data/smart contracts* | ▶ Lagere graad van distributie van vertrouwen<br>▶ Vaak hogere operationele complexiteit |
| *Geavanceerde cryptografie* | ▶ Hogere technologische complexiteit<br>▶ Meer rekenkracht en opslag vereist<br>▶ Vaak toepassingsspecifiek |

Blockchain laat toe afhankelijkheden van intermediaire partijen te reduceren. Niet langer een vertrouwde partij bewaart als enige data, garandeert eigenschappen over data of voert regels uit, maar het blockchainnetwerk zelf. De prijs die men ervoor betaalt, is een verlies van confidentialiteit door transparantie, in die zin dat meerdere entiteiten toegang tot bepaalde informatie nodig hebben in het validatieproces. Tot op heden zijn er geen generieke blockchainoplossingen die deze uitdagingen op een voldoende praktische manier aanpakken. Het is dan ook afwachten wat de toekomst brengt.

## 7.5. Het blockchaintrilemma

Bij blockchain blijkt aldus een spanningsveld te bestaan tussen drie concepten: veiligheid, schaalbaarheid en distributie van vertrouwen. Als we één van deze drie aspecten verbeteren, gaat dit ten koste van minstens één van de andere aspecten[376].

376 K. Verslype, 'Blockchain & gedistribueerd vertrouwen – Deel 3/3: Het blockchain trilemma', *Smals research*, 18 september 2018, www.smalsresearch.be/blockchain-gedistribueerd-vertrouwen-deel-3-het-blockchain-trilemma.




Figuur 14. Het blockchaintrilemma.

Wat betekenen deze drie termen?

– *Distributie van vertrouwen*
  Dit is het aantal participanten dat betrokken is in het consensusmechanisme en de graad waarin hun macht evenredig verdeeld is. Of anders geformuleerd: het aantal partijen dat verifieert of de regels gerespecteerd worden. De vraag daarbij is ook of de stem van elk van die participanten even zwaar doorweegt en of de participanten effectief onafhankelijk van elkaar opereren.
– *Schaalbaarheid*
  Dit betreft het aantal transacties dat per seconde door het netwerk verwerkt kan worden.
– *Veiligheid*
  Veiligheid bestaat uit diverse aspecten. Traditioneel spreekt men over CIA, wat staat voor *confidentiality*, *integrity* en *availability* (*i.e.* confidentialiteit, onwijzigbaarheid en beschikbaarheid). Blockchaintechnologie scoort slecht op het vlak van confidentialiteit, goed op het vlak van onwijzigbaarheid, en, afhankelijk van de invalshoek, goed of slecht op het vlak van beschikbaarheid. Wat betreft die beschikbaarheid, is er enerzijds geen *single point of failure* (SPOF), maar anderzijds zal in een traditionele blockchainbenadering de participant zijn geheime sleutel zelf moeten beschermen om zijn op de blockchain geregistreerde activa ter beschikking te houden.

Het is momenteel bijzonder moeilijk, misschien zelfs onmogelijk, om tot een technologische oplossing te komen die op de drie punten tegelijk sterk scoort. Eigenlijk is dit niet onlogisch. Men kan niet alle participanten in een groot, druk netwerk de verantwoordelijkheid geven om constant alles te valideren. Dit hoeft geenszins te betekenen dat blockchaintechnologie onbruikbaar is, maar wel dat ze fundamentele beperkingen heeft. Het kan een domper zetten op de idee dat er voor platformen met enorm hoge volumes, zoals eBay en Facebook, sterk gedistribueerde en tegelijkertijd zeer veilige

alternatieven mogelijk zijn. Het zal erop aankomen om per toepassing te zoeken naar het juiste evenwicht.

## 7.6. **Beyond blockchain**

Blockchaintechnologie is een familie van technologieën die onderliggend gebaseerd zijn op hetzelfde principe, al bestaan onderling grote verschillen. Blockchaintechnologieën behoren dan weer zelf tot de grotere familie van de *Distributed Ledger Technology* (DLT), waarbij het onderliggende principe is dat een datastructuur waar enkel gegevens aan toegevoegd kunnen worden (de *ledger*), collectief gedeeld en veilig gehouden wordt. Voorbeelden van DLT's die geen blockchain zijn, zijn het al vermelde IOTA en CORDA.

Misschien willen we enkel onwijzigbare data delen zonder daarbij afhankelijk te zijn van een centrale dienst. Ook in zulk geval zullen velen kijken in de richting van blockchain. Toch is blockchain niet onmiddellijk sowieso de beste keuze, aangezien de data nooit verwijderd kunnen worden en vele entiteiten een volledige kopie van de blockchain moeten bijhouden. Er is in dit kader een veel minder gekende technologie die luistert naar de naam *Distributed Hash Tables* (DHT's). De twee technologieën kunnen eventueel ook gecombineerd worden: in een afgeschermd, *permissioned* blockchainnetwerk kunnen *fingerprints* van data geregistreerd worden, die door middel van DHT's en vercijfering veilig en bijkomend in het netwerk opgeslagen worden.

Al voordat Bitcoin in 2009 gelanceerd werd, bestonden er cryptografische technologieën om noodzakelijk vertrouwen in bepaalde partijen te reduceren. De focus lag echter op confidentialiteit, daar waar blockchain net steunt op transparantie. Enkele voorbeelden die hierna geïllustreerd worden, zijn *multi-party computation*, *n-m secret sharing, zero-knowledge proofs* en *attribute-based credentials*.

*- Multi-party computation (MPC)*[377]

Stel: een groep vrienden wil te weten komen wat hun gemiddelde loon is, zonder dat één van hen zijn loon wil prijsgeven. Dit kan met behulp van *multi-party computation* opgelost worden. Het is een gedistribueerd protocol, waarbij iedereen zijn loon als input geeft aan zijn MPC-software. Het enige wat de participanten van elkaar leren, is het gemiddelde loon. Er is verder dus geen informatie die lekt. We vertrouwen elkaar niet voldoende om elkaars loon te mee te delen, maar wel voldoende opdat iedereen de correcte input geeft. MPC werd al theoretisch voorgesteld in de jaren 1980. Het laat toe om collectief een functie te berekenen, code uit te voeren waarbij de input van de verschillende partijen confidentieel blijft. Dit staat in sterk contrast met de op transparantie steunende blockchainbenaderingen.

377 O. Goldreich, *Secure multi-party computation*, manuscript (preliminary version 78), 1998.

*- N-m Secret Sharing*[378]
Dit werd al in 1979 uitgevonden. Het idee is dat je een geheim, zoals een wachtwoord of een private cryptografische sleutel, opsplitst in *n* stukken. Eén stuk op zich geeft geen informatie prijs, maar zodra een persoon een bepaald aantal (*m)* stukken heeft, kan die opnieuw het geheim samenstellen. Een burger kan een geheim bijvoorbeeld in drie stukken knippen (n=3), waarbij hij één stuk thuis bewaart, het tweede stuk op zijn werk en het derde stuk in zijn kluis in de bank. Stel dat de persoon in dit geval met twee stukken voldoende heeft om het geheim opnieuw samen te stellen (m=2). Wanneer een stuk gestolen wordt, kan de dief of vinder daar geen nuttige informatie uit afleiden. Als er één stuk verloren gaat of gestolen wordt, is dit dus geen probleem.

*- Zero-knowledge proofs*[379]
Deze technologie laat toe om te bewijzen dat je een geheim (een bepaalde waarde) kent, zonder verdere informatie over het geheim (die waarde) prijs te geven. Een heel simpel voorbeeld is een digitale handtekening: men bewijst dat men de eigenaar is van de private sleutel, zonder die sleutel zelf prijs te geven. Men kan ook verdergaan: men kan eigenschappen bewijzen over dat geheim, bijvoorbeeld dat het zich binnen bepaalde waarden bevindt, of dat het deel uitmaakt van een gekende set van waarden. Deze technologie vinden we ook terug in een aantal blockchaintechnologieën.

*- Attribute-based credentials*[380]
Dit zijn complexe *zero-knowledge proofs* die de privacy van de burger kunnen helpen beschermen, door hem meer controle te geven over de persoonsgegevens die prijsgegeven worden aan een andere partij, zoals een webshop. Dit werkt als volgt: een autoriteit reikt aan de burger een speciaal certificaat uit. Dit certificaat bevat persoonsgegevens zoals geboortedatum en adres. Wanneer de burger zich wil authentiseren naar een andere partij, heeft hij fijnkorrelige controle over wat hij prijsgeeft. Hij zou bijvoorbeeld enkel kunnen bewijzen dat hij ouder is dan achttien jaar en in de provincie Noord-Brabant woont. Dat bewijs wordt lokaal op de computer van de burger gecreëerd op basis van het certificaat, zonder medewerking van een of andere autoriteit. De verifieerder leert op basis van dat bewijs enkel dat de handtekening geplaatst werd door een volwassen inwoner van Noord-Brabant en dat de correctheid van deze gegevens gegarandeerd wordt door een bepaalde autoriteit, zoals de Rijksdienst voor Identiteitsgegevens (RvIG) van het Nederlandse Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Het certificaat zelf blijft dus geheim, maar enkel daaruit afgeleide bewijzen worden prijsgegeven. De burger kan ook verhinderen dat een bewijs aan één van zijn vorige bewijzen gekoppeld kan worden. Wanneer de burger zich meermaals bij dezelfde webshop authentiseert, weet de webshop op basis van de bewijzen dan niet

378 A. Shamir, 'How to share a secret', *Communications of the ACM* 1979, vol. 22, nr. 11, 612-613.
379 U. Feige, A. Fiat & A. Shamir, 'Zero-knowledge proofs of identity', *Journal of cryptology* 1988, vol. 1, nr. 2, 77-94.
380 K. Rannenberg, J. Camenisch & A. Sabouri, *Attribute-based Credentials for Trust – Identity in the Information Society*, Berlijn, Springer, 2015.

dat het over dezelfde persoon gaat. De technologie kan niet alleen voor authenticaties gebruikt worden, maar evengoed voor het plaatsen van digitale handtekeningen. De verifieerder van de handtekening leert dan enkel dat de handtekening geplaatst werd door een meerderjarige uit Noord Brabant.

- *Verifiable encryption*[381]

Deze technologie laat toe eigenschappen over vercijferde data te bewijzen. Stel dat Alice een bedrag encrypteert met de publieke sleutel van Bob. Enkel Bob kan dat decrypteren. Toch is Alice in staat aan Charlie te bewijzen dat het bedrag binnen bepaalde waarden ligt.

Er is dus al meer beschikbaar dan blockchain om minder afhankelijk te worden van bepaalde autoriteiten of om gevoelige (persoons)gegevens te beschermen. Blockchain is op dit moment zonder twijfel de technologie die de meeste aandacht krijgt. Enerzijds blijven door de hype rond blockchain andere waardevolle technologieën echter een beetje in de schaduw. Anderzijds kunnen de technologieën ook elkaar versterken. Zcash en Sovrin steunen bijvoorbeeld uitgebreid op *zero-knowledge proofs* en *n-m secret sharing* kan gebruikt worden om de sleutel te beschermen die toegang geeft tot iemands virtuele munten. Het kan wel een uitdaging zijn om alles voldoende performant te houden.

Het moet, ten slotte, ook gezegd worden dat net dankzij de blockchainhype er een toegenomen interesse is in cryptografie en dat er in de praktijk niet zelden een combinatie van meerdere technologieën nodig zal zijn. Deze toegenomen aandacht is al een mooie verdienste van de blockchaintechnologie.

381 J. Camenisch & V. Shoup, 'Practical verifiable encryption and decryption of discrete logarithms' in D. Boneh (ed.), *Advances in Cryptology – CRYPTO 2003*, Berlijn, Springer, 2003, p. 126-144.

# 8. Lessen uit het verleden

Het is oktober 1969. Charlie Kline bevindt zich in de University of California Los Angeles (UCLA). Zijn collega Bill Duvall, eveneens een jonge programmeur, is op datzelfde moment in het Stanford Research Institute (SRI). Ze slagen er voor het eerst in een bericht te versturen over ARPANET, een gedistribueerd en robuust netwerk waar een paar jaar later het TCP/IP-protocol uit zou ontstaan. Het hele internet is tot op vandaag op dit protocol gebouwd. ARPANET liet toe om berichten te versturen over een netwerk dat exclusief bestaat uit knooppunten die onbetrouwbaar zijn, in de zin dat ze op elk moment konden uitvallen. Een dergelijk netwerk was niet afhankelijk van een centraal knooppunt en kon zelfs een nucleaire aanval overleven, wat in de Koude Oorlog een sterk pluspunt was.

De echo's uit de jaren 1960 zijn onmiskenbaar als we kijken naar blockchain. Door middel van een gedistribueerd netwerk kan robuust en zonder afhankelijkheid van een centrale partij informatie of activa uitgewisseld worden. Vaak wordt gesteld dat blockchain en meer algemeen *Distributed Ledger Technology* (DLT) even belangrijk zal worden als internet zelf. Daar waar internet het uitwisselen van informatie snel en goedkoop maakte, zou DLT vooral het uitwisselen van alles van waarde snel en goedkoop maken. We zouden daarvoor niet langer afhankelijk zijn van een centrale autoriteit zoals een bank, notaris of overheid, maar zal gebeuren op een robuust, gedistribueerd blockchainnetwerk dat via internet draait. De vraag is echter of alles wel zo'n vaart zal lopen. Laat ons daarvoor eens naar de evolutie van internet zelf kijken.

Boven op het gedistribueerde internet werden heel wat gecentraliseerde of hiërarchische top-downdiensten gebouwd. Midden jaren 1980 ontstond *DNS (Domain Name Service)*, waardoor we niet langer de IP-adressen van computers hoeven te kennen, maar enkel de domeinnaam. We hoeven dus niet langer *74.125.224.72* te onthouden, maar gewoon *google.com*. Als we over een veilig kanaal naar een website surfen of een digitale handtekening willen verifiëren, maken we gebruik van een *PKI* (*Public Key Infrastructure*), wat eveneens een hiërarchische top-downdienst is die al begin jaren 1970 ontwikkeld werd. Dankzij een PKI weten we met wie we communiceren, maar daarvoor moeten we die PKI wel vertrouwen.

Begin 1990 werd *HTTP* (*Hypertext Transfer Protocol*) geïntroduceerd, wat de creatie van websites toeliet. Hoe vinden we echter de juiste website? In 1996 zetten twee studenten aan Stanford University, Larry Page en Sergey Brin, een zoekmachine op die luisterde naar de naam *Google*. Hun bedrijf groeide snel uit tot een wereldspeler.

De ontwikkeling van nieuwe technologieën liet vanaf de eerste jaren van dit millennium toe om het idee van het Web 2.0 te realiseren, waarbij de nadruk voortaan zou

liggen op interactiviteit en door de burgers zelf gecreëerde inhoud, wat in scherp contrast stond tot de voorheen statische websites. Ook toen hoorden we stemmen opgaan dat de oligopoliepositie van mediabedrijven zou verdwijnen en de democratie hoogtij zou vieren. Iedereen wordt redacteur van nieuws en iedereen wordt auteur dankzij de nieuwe kanalen. We zouden niet langer afhankelijk zijn van mediabedrijven die we moeten vertrouwen voor accurate informatie en representatieve berichtgeving. In 2003 lanceerde Mark Zuckerberg, een student aan de Harvard University, *Facemash*. Wegens schendingen van de auteursrechten en privacy moest *Facemash* al snel offline gehaald worden, maar Zuckerberg werkte desondanks verder aan zijn project en lanceerde in 2004 *Facebook*. Dit was enkel mogelijk dankzij het Web 2.0, wat naast Facebook ook het ontstaan mogelijk maakte van een heel aantal andere grote sociale platformen zoals *LinkedIn, YouTube* en *Twitter*. Het zijn echter de bedrijven achter deze platformen die bepalen wat gecensureerd wordt, wat u te zien krijgt en die soms een loopje nemen met uw privacy. Iedereen is dus auteur, maar weliswaar onder strikte supervisie. Bij onrust in landen zoals Turkije en Egypte wordt toegang tot dergelijke platformen op kritische momenten door de overheid overigens gewoon geblokkeerd. Recent zien we ook nog de proliferatie van *fake news*, waarvan de verspreiding door middel van deze sociale media gefaciliteerd wordt. Centrale platformen bepalen in toenemende mate wat echt en wat *fake* nieuws is. De burger als leverancier van data klinkt zeer gedistribueerd. In de praktijk zien we echter tegelijkertijd een sterke centralisatiebeweging.

Dit zijn een aantal voorbeelden die aangeven dat er op dit moment niet veel meer overblijft van het gedistribueerde karakter van internet. Het kan paradoxaal klinken, maar de gedistribueerde basislaag van internet heeft net de condities gecreëerd voor gecentraliseerde wereldspelers zoals Facebook en Google.

Dit alles leert ons dat de idee of de belofte van publieke gedistribueerde netwerken, waarbij de macht opnieuw komt te liggen bij de individuele participanten en waarbij centrale spelers niet langer nodig zouden zijn, niets nieuws is onder de zon. Het verleden leert ons dat er in de praktijk vaak ook tegelijkertijd een centralisatiebeweging plaatsvindt. Of anders geformuleerd: de intentie tot distributie, die mogelijk wordt dankzij technologische evoluties, resulteert *de facto* in nieuwe vormen van centralisatie.

De vraag is nu of dit voor de blockchaintechnologie ook het geval zal zijn. Voor Bitcoin zien we opnieuw deze beweging. Bitcoin zou de democratie verhogen, zo werd beloofd. We hoorden slogans zoals '*democratisering van het geld*' en '*banking the unbanked*'. Centrale en andere banken zouden verdwijnen, want burgers zouden voortaan hun eigen geld kunnen creëren en transfereren. De werkelijkheid is evenwel dat er paar nieuwe machtscentra ontstaan zijn, *mining*bedrijven en *miningpools*, die zich aan controle onttrekken[382]. Vanuit democratisch perspectief is dat een stap achteruit in vergelijking met het bestaande systeem. Daarnaast zijn er nog de handelsplatformen en aan-

382 G. Honsel, 'Zentralisierung statt Demokratisierung: Neue Hierarchien durch die Blockchain', Heise Online, 21 september 2017, www.heise.de/newsticker/meldung/Zentralisierung-statt-Demokratisierung-Neue-Hierarchien-durch-die-Blockchain-3835702.html.

bieders van onlinewallets waar we afhankelijk van zijn. Bovendien is ook de Bitcoin-rijkdom erg sterk geconcentreerd: bijna één derde van alle bitcoins is eigendom van 1.600 pseudoniemen[383]. Dit geeft een paar mensen de mogelijkheid om koersen te manipuleren ten nadele van alle anderen. Bovendien is dit handvol personen niet aan (politieke) controle onderhevig, zoals dat bij de centrale banken wel het geval is. Over blockchain en *Distributed Ledger Technology* (DLT) zijn gelijkaardige optimistische geluiden te horen, zoals: '*Blockchain biedt mogelijk de infrastructuur voor een rechtvaardige, inclusieve, veilige en democratische digitale economie*'[384]. De vraag is echter in welke mate publieke blockchainnetwerken zullen kunnen weerstaan aan de dynamiek tot centralisering die we tot nu toe zagen.

Wanneer nieuwe virtuele munten of gedistribueerde applicaties gelanceerd worden, die van DLT gebruikmaken, houden de makers een aanzienlijk deel van de muntjes of tokens voor zichzelf. Daardoor krijgen ze naast rijkdom ook disproportioneel veel zeggenschap over blockchains, gebaseerd op *Proof of Stake* of *Distributed Proof of Stake*. Daarnaast zullen de bedrijven vaak de controle over de ontwikkeling van de code, alsook de controle over het smart contract bij hen houden, zoals het geval is bij de gedistribueerde toepassing *CryptoKitties*. Het bedrijf achter *CryptoKitties* heeft weliswaar geen controle over de uitvoering van het smart contract, maar heeft wel een mechanisme voorzien dat toelaat het smart contract te vervangen door een ander. Stel dat er bijvoorbeeld ooit een gedistribueerd alternatief voor booking.com ontstaat op een blockchain, dan is er een goede kans dat dit dus nog steeds gecontroleerd zal worden door één bedrijf.

*A fortiori* bij afgeschermde blockchainnetwerken zien we ook vormen van centralisering ontstaan. De noodzaak aan vertrouwen verdwijnt dus niet, maar wordt geherlokaliseerd zodat samenwerking gefaciliteerd en gestimuleerd wordt tussen een beperkte groep participanten die elkaar kennen maar toch wantrouwen. In afgeschermde blockchainnetwerken zullen de verschillende participanten bovendien contractueel verbintenissen moeten aangaan. Ook dit maakt vertrouwen in centrale partijen noodzakelijk, zelfs in een blockchainwereld. Zo zullen criteria afgesproken worden met betrekking tot onder meer veiligheid, beschikbaarheid en reactietijd van de systemen bij de verschillende participanten. Ook het smart contract zal aan bepaalde criteria moeten voldoen, bijvoorbeeld met betrekking tot veiligheid en functionaliteit. Het creëren van vertrouwen dat aan al die criteria voldaan is, zal ons inziens audits noodzakelijk maken door een vertrouwde externe partij. Afspraken en verantwoordelijkheden zullen onderling vastgelegd moeten worden. In het kader van de Algemene Verordening Gegevensbescherming moeten bijvoorbeeld het doel en de middelen van de verwerking van de persoonsgegevens bepaald worden, en moet afgesproken worden wie verantwoordelijk is voor welke verplichting, in het bijzonder het informeren. Dit alles sluit niet uit dat het alsnog verkeerd loopt of dat er geschillen ontstaan. In dat geval moeten de

383 H. Murphy, 'Bitcoin whales' control third of market with $37.5bn holdings', Financial Times, 9 juni 2018, www.ft.com/content/c4b68aec-6b26-11e8-8cf3-0c230fa67aec.

384 Zie 'The trust machine – The promise of the blockchain', The Economist, 31 oktober 2015, www.economist.com/leaders/2015/10/31/the-trust-machine.

participanten alsnog naar de rechter kunnen stappen die te allen tijde een effectieve rechtsbescherming moet kunnen bieden.
Een voorbeeld van een dergelijk afgeschermd blockchainnetwerk, dat op het moment van schrijven weliswaar nog in de steigers staat, is Libra. Met Libra tracht Facebook een eigen *stable coin* te creëren. Het zou beheerd en veilig gehouden worden door een twintigtal bestaande bedrijven waaronder Uber, Spotify en Vodafone[385]. Als de Libra er ooit komt, dan zul je als burger de dienst enkel kunnen consumeren. Van participeren is geen sprake meer. Het enige dat je als burger misschien nog zal kunnen aanleveren, is data voor nog meer doelgerichte reclame.
De toekomst zal dus niet enkel uitwijzen in welke mate DLT een rol zal spelen in onze bredere samenleving, maar ook onder welke vorm. Indien we vlot waarden willen kunnen uitwisselen en tegelijkertijd risico's, zoals verlies van de geheime sleutel, voldoende willen afdekken, dan is centralisatie van bepaalde aspecten wellicht een noodzaak. Zo kan het zeker aangeraden zijn om bij vastgoedtransacties een rol te behouden voor de notaris (*supra* hoofdstuk 4, Blockchain en vastgoed).
Een wereld waarin al het vertrouwen evenredig gedistribueerd is over alle betrokkenen en waarbij geen nood meer is aan vertrouwde entiteiten, is dus niet voor morgen. Misschien moeten we tot de vaststelling komen dat het de initiële doelstelling van blockchain eigenlijk niet de juiste was. Deze luidde: '*Hoe kunnen we een autoriteit, die we verplicht zijn te vertrouwen, elimineren?*' Die vraag moeten we in vele gevallen eigenlijk vervangen door: '*Kan technologie processen optimaliseren evenals het noodzakelijke vertrouwen, al dan niet met een noodzakelijke controlerende rol voor autoriteiten, waarborgen?*' Ook bij deze vraag kan een verdere ontwikkeling van DLT wellicht een bijzonder waardevolle rol spelen. Vertrouwde autoriteiten, zoals overheden, banken en notarissen, zullen dus blijven bestaan, maar hun rol zal wel herijkt worden.

385 S. Klebnikov, 'Here Are All The Companies That Bailed On Facebook's Libra', *Forbes*, 21 oktober 2019. https://www.forbes.com/sites/sergeiklebnikov/2019/10/21/here-are-all-the-companies-that-bailed-on-facebooks-libra/.